NASA Conference Publication 10011

CARE III Users' Workshop

Compiled by
Research Triangle Institute
Research Triangle Park, North Carolina

Proceedings of a workshop sponsored by the National Aeronautics and Space Administration, Washington, D.C., and held at Langley Research Center Hampton, Virginia October 6-7, 1987

(NASA-CP-10011) CARE 3 USER'S WORKSHOP N88-21646
(NASA) 160 p CSCL 12A

Unclas
G3/59 0130162

National Aeronautics and Space Administration

INTRODUCTION

A users' workshop for CARE III, a reliability assessment tool designed and developed especially for the evaluation of high-reliability fault-tolerant digital systems, was held at NASA Langley Research Center in Hampton, Virginia on October 6 and 7, 1987.

The main purpose of the workshop, sponsored by co-chairmen Salvatore J. Bavuso (NASA-LaRC) and Anna L. Martensen (PRC Kentron, Inc.), was to assess the evolutionary status of CARE III — or, as Sal Bavuso put it, "where do we go from here?"

The workshop opened with Chuck Meissner, branch head of the Systems Validation Methods Branch, welcoming the 19 attendees from 13 different companies and giving them an overview of NASA-LaRC. Sal Bavuso followed with an introduction and history of CARE III, with Roberto E. Altschul of Boeing Electronics Company discussing its mathematical theory. The rest of the first day and half of the second day were devoted to discussions and presentations by attendees and members of NASA-LaRC. Features and limitations of CARE III, and comparison to other tools were the main topics. Copies of the presentations follow this introduction.

A tour of AIRLAB began on the second day with an overview of the facility by Chuck Meissner. The attendees alternated among three different stations in which there were discussions and demonstrations of the Semi-Markov Unreliability Range Evaluator (SURE) by Ricky Butler, Fault Injection by George Finelli, and Software Reliability by Jon Sjogren. The final hours of the workshop were devoted to hands-on demonstrations and tutorials of CARE III and HARP.

The results of a questionnaire filled out by the attendees helped to address recommendations for future enhancement of CARE III. A summary of the responses follows:

1. Weibull is frequently used for long mission times.
2. Some users compute steady-state availability with CARE III.
3. Many users do both steady state and instantaneous availability.
4. Most users believe CARE III can model very large systems and most don't know of another program that can handle fault tree applications.
5. All users consider CARE III to be valuable enough to warrant continued development.
6. A number of components in fault-tolerant systems can vary from about 15 to 3,000, depending upon the complexity of the system.
7. Most execution times for CARE III range from 5 to 10 minutes.
8. Most users responded "confident" to "very confident" in using CARE III (none responded "skeptical" or "not-confident").
9. Testing of CARE III is thought to be adequate to very well.

10. One user discovered a method of approximating the effects of state dependent coverage.
11. One user suggested using the Weibull distribution to approximate dormant spares.
12. All the stated applications are aerospace.
13. Sequence and state dependency modeling are common.
14. Some users typically use the CARE III FEHM and think it is not powerful enough, while others say it is too complicated and don't use it.
15. No user suggested a method of doing sequence dependency with CARE III.
16. Some use the CARE III menu and some don't.

In conclusion, the CARE III program is considered to be very flexible and useful. A recurrent theme throughout the workshop, however, was the suggestion that one should use more than one tool at a time when analyzing complex systems. An overall interest in CARE III was indeed displayed by all of the attendees.

THE CARE III THEORY IMPLEMENTATION AND CODE

October 6, 1987

Anna L. Martensen

PRC Kentron, Inc.

Behavioral Decomposition

FORM - Fault Occurrence/Repair Model
Describes fault arrivals

FEHM - Fault/Error Handling Model
Describes the fault handling characteristics of a system

With this decomposition technique, the time separations between FORM and FEHM are recognized

PRECEDING PAGE BLANK NOT FILMED

The Fault Occurrence/Repair Model

System components are described as modules

Like modules comprise a stage

A stage may have one or more modules

System failure due to hardware depletion is described by a fault tree
- CARE III fault tree allows for common mode events

Fault/Error Handling Model

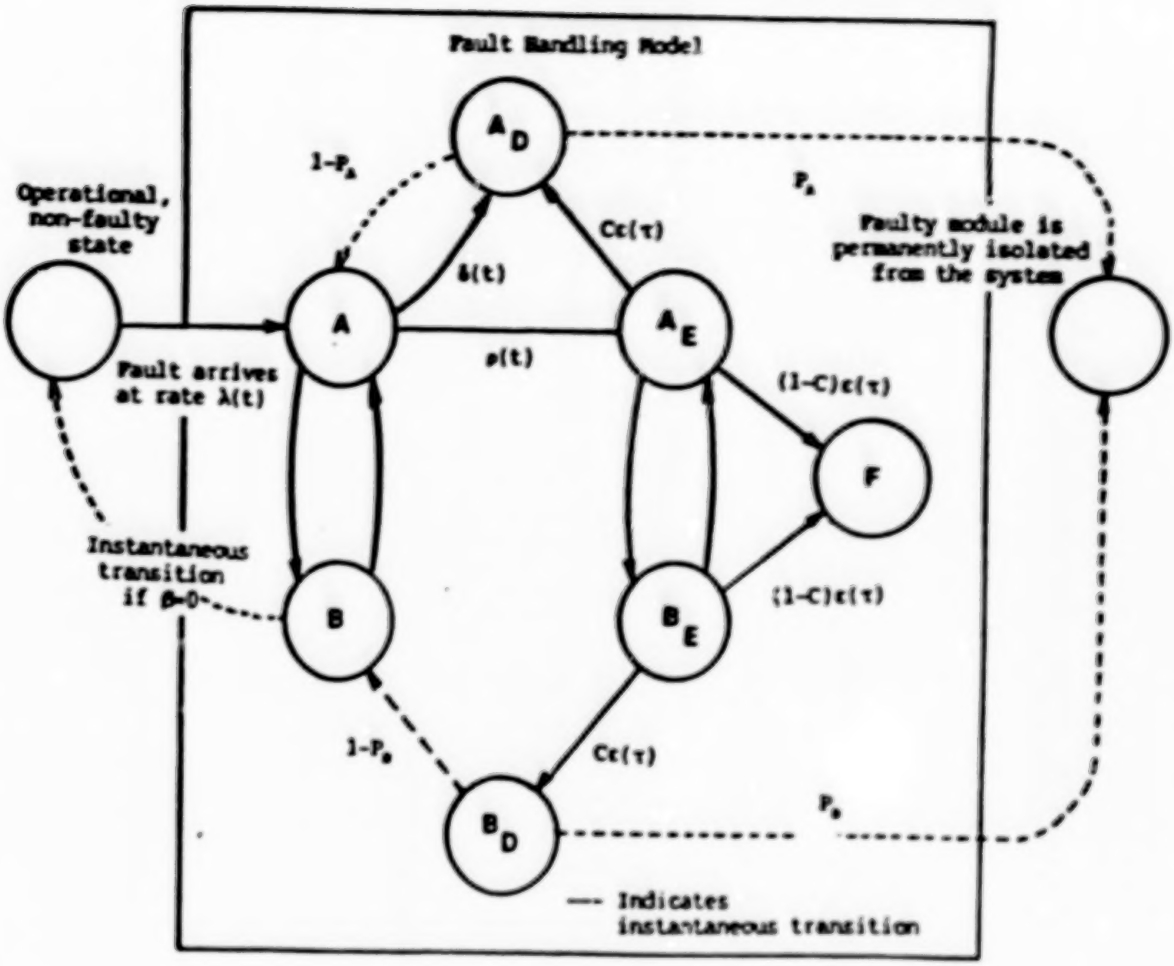
CARE III single fault model

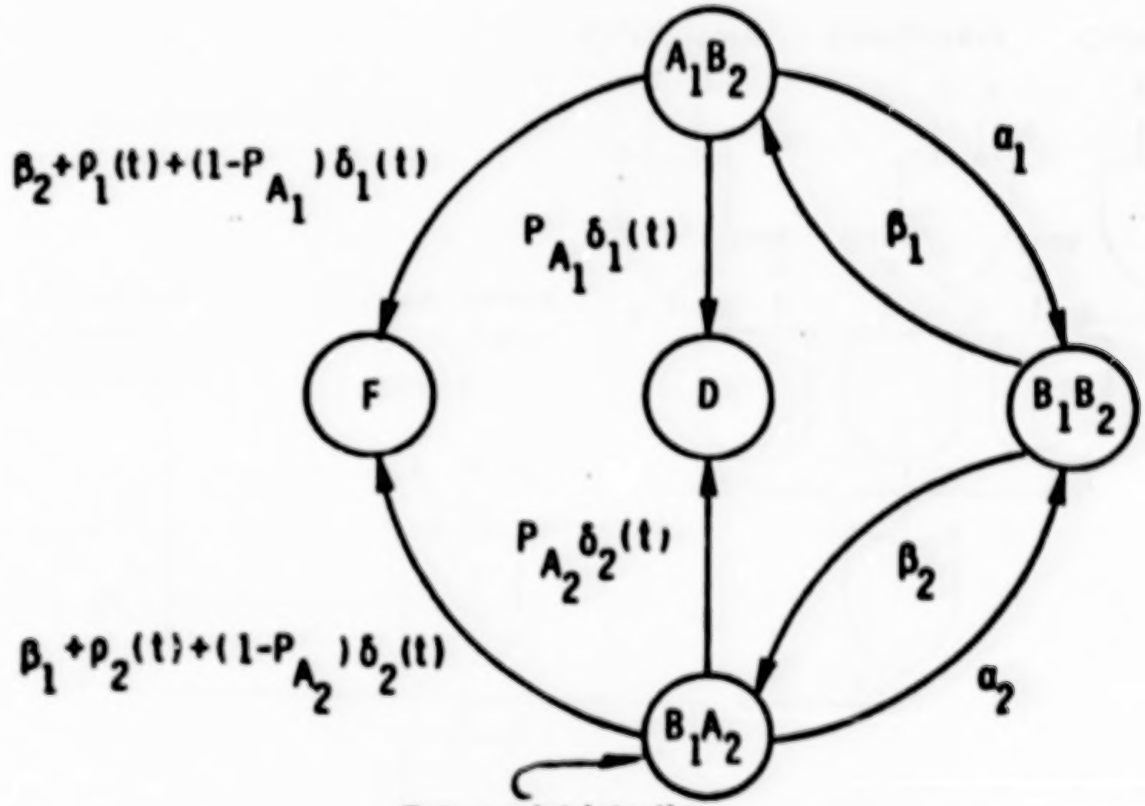
CARE III double fault model

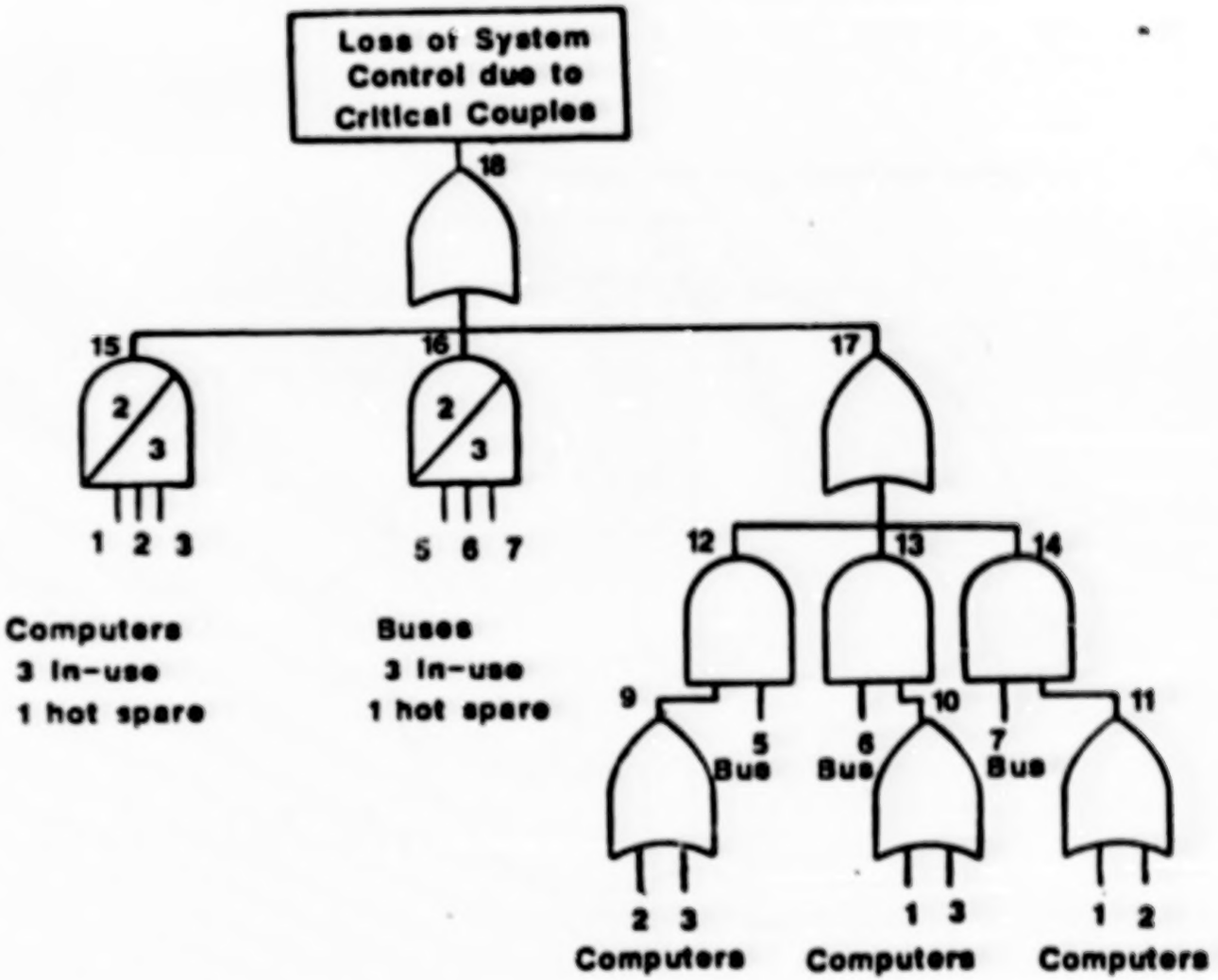
- unless the first fault is benign when the second fault arrives, the two "near-coincident" faults are assumed to cause system failure
  NOTE: Critical pairs must be specified in the CARE III input file

- if the first fault is benign, the CARE III double (intermittent) fault model is entered

ORIGINAL PAGE IS
OF POOR QUALITY




A_1B_2
B_1B_2
B_1A_2
F
D
$\beta_2+\rho_1(t)+(1-P_{A_1})\delta_1(t)$
$P_{A_1}\delta_1(t)$
α_1
β_1
$P_{A_2}\delta_2(t)$
β_2
$\beta_1+\rho_2(t)+(1-P_{A_2})\delta_2(t)$
α_2
Entry point into the
Double Intermittent Fault Coverage Model


Loss of System Control due to Critical Couples
18
15
16
17
2
3
2
3
1 2 3
5 6 7
Computers
3 in-use
1 hot spare
Buses
3 in-use
1 hot spare
12
13
14
9
10
11
5 Bus
6 Bus
7 Bus
2 3
1 3
1 2
Computers
Computers
Computers

CARE III Input File

There are six parts to a CARE III input file:

- fault handling models
- stage descriptions
- FEHM-to-stage assignment
- Misc. to include mission time and algorithm control parameters
- the system tree (optional)
- the critical pair tree (optional)

```
$FHDNAMES
     FHDNAME(1)= '(NONE)',
     FHDNAME(2)= 'PERMANENT C',
     FHDNAME(3)= 'PERMANENT B'
$END
$FLTTYP
     NFTYPS=3,
     ALP=      0.0    ,      0.0    ,      0.0    ,
     BET=      0.0    ,      0.0    ,      0.0    ,
     DEL=  '3600.0    ,    360.0    ,  10000.0    ,
     RHO=      0.0    ,    180.0    ,      0.0    ,
     EPS=      0.0    ,   3600.0    ,      0.0    ,
     IDELF=      1    ,      1      ,      1      ,
     IRHOF=      1    ,      1      ,      1      ,
     IEPSF=      1    ,      1      ,      1      ,
     MARKOV=     1    ,
     PA=       1.0    ,      1.0    ,      1.0    ,
     PB=       1.0    ,      0.0    ,      0.0    ,
     C=        1.0    , 9.990000E-01,      1.0    ,
     LGTMST=T
$END
$STGNAMES
     STGNAME(1)= 'INERTIAL REF',
     STGNAME(2)= 'PITCH RATE',
     STGNAME(3)= 'COMPUTER',
     STGNAME(4)= 'SECONDARY ACT',
     STGNAME(5)= 'COMPUTER BUS'
$END
$STAGES
     NSTGES=5,
     N =  3,  3,  4,  3,  4,
     M =  2,  2,  2,  2,  2,
     NSUB=  0,  0,  0,  0,  0,
     MSUB=  0,  0,  0,  0,  0,
     LC=  0,  0,  0,  0,  0,
     NOF(1,3)=3,
     NOP(1,5)=3,
     IRLPCD=1,
     RLPLOT=F,IAXSRL=2
$END
$FLTCAT
     NFCATS=1,1,1,1,1,
     JTYP(1,1)=  1,
     JTYP(1,2)=  1,
     JTYP(1,3)=  2,
     JTYP(1,4)=  1,
     JTYP(1,5)=  3,
     OMG(1,1)=       1.0    ,
     OMG(1,2)=       1.0    ,
     OMG(1,3)=       1.0    ,
     OMG(1,4)=       1.0    ,
     OMG(1,5)=       1.0    ,
```

```
      RLM(1,1)= 1.500000E-05,
      RLM(1,2)= 1.900000E-05,
      RLM(1,3)= 4.800000E-04,
      RLM(1,4)= 3.700000E-05,
      RLM(1,5)= 2.700000E-06
$END
$SRVTIME
      FT=  10.0000    ,ITBASE=1,
      PCTRNC= 0.100000E-09,
      QCTRNC= 0.100000E-01,
      NPSBRN=20,
      CKDATA=T,
      SYSFLG=T,CPLFLG=T
$END
SYSTEM TREE EX 7
1 5 6 6
6  O 1 2 3 4 5
CRITICAL PAIRS TREE EX 7
1 8 9 18
3 1 4
5 5 8
9  O 2 3
10  O 1 3
11  O 1 2
12  A 9 5
13  A 10 6
14  A 11 7
15  2 1 2 3
16  2 5 6 7
17  O 12 13 14
18  O 15 16 17
```

The CARE III Program

Three primary program modules:

- CINAME/CAREIN
- COVRGE
- CARE3

Additional plotting programs:

- RELPLT*
- CVGPLT*

CARE III command files

- RUNCARE
- RUNPLOT

CAREIN/CINAME

Reads the CARE III input file

Checks the input file

Finds component configurations that represent system failure (fault tree analysis)

- CAREINORIG
- CAREIN (new)

Example: 0 represents fail
1 represents operational

1 1 1 1
0 1 1 1
1 0 1 1
1 1 0 1
1 1 1 0
etc.

COVRGE

Solution of the CARE III coverage model requires

- numerical sum of 2 functions
- numberical integration of 2 functions (Simpson's Rule)
- numerical convolution of 2 functions (Trapezoidal Rule)
- numerical solution of Volterra equations (Based on Trapezoidal Rule)

CARE3

Computes QSUM and P*SUM values using information from the CAREIN and COVRGE program modules

Prints results

Solution of the CARE III model requires
- Integration (Simpson's Rule)
- Convolution
- Combinatorics

INTRODUCTION TO THE CARE III MATHEMATICAL MODEL

October 6, 1987

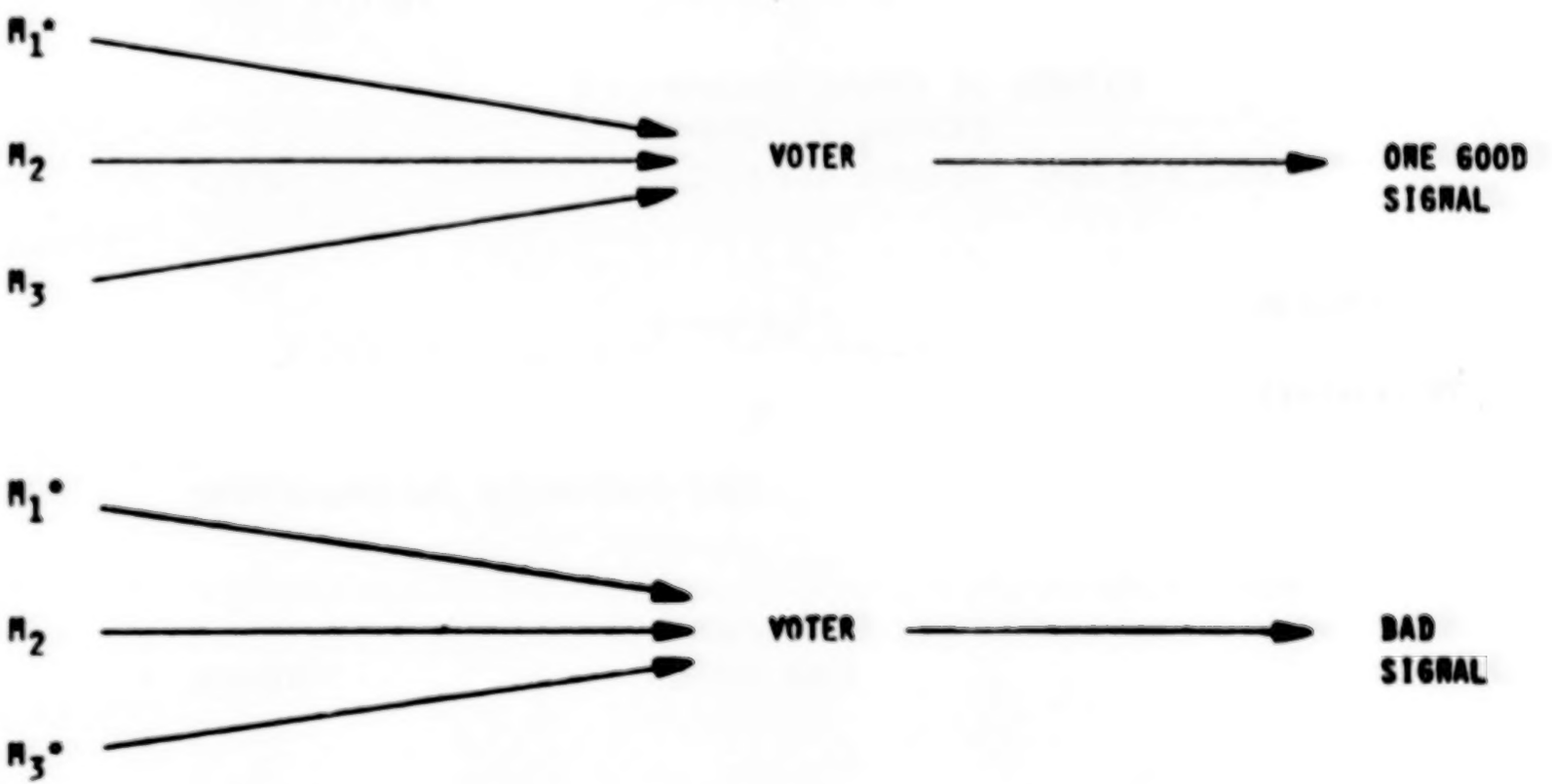
Roberto E. Altschul

Boeing Electronics Company

CLASSICAL MODEL

- REDUNDANCY
- FAULT TOLERANCE (PERFECT FAULT-HANDLING ABILITY TO MASK FAULT UNTIL DETECTION, RECONFIGURATION

MASKED REDUNDANCY



- MODULE: BASIC UNIT
  INDEPENDENT FAILURES

MODULE FAILURE OCCURRENCE RATE

$$\lambda(t) = \begin{cases} \lambda & \text{EXPONENTIAL} \\ \lambda\omega(\lambda t)^{\omega-1} & \text{WEIBULL} \end{cases}$$

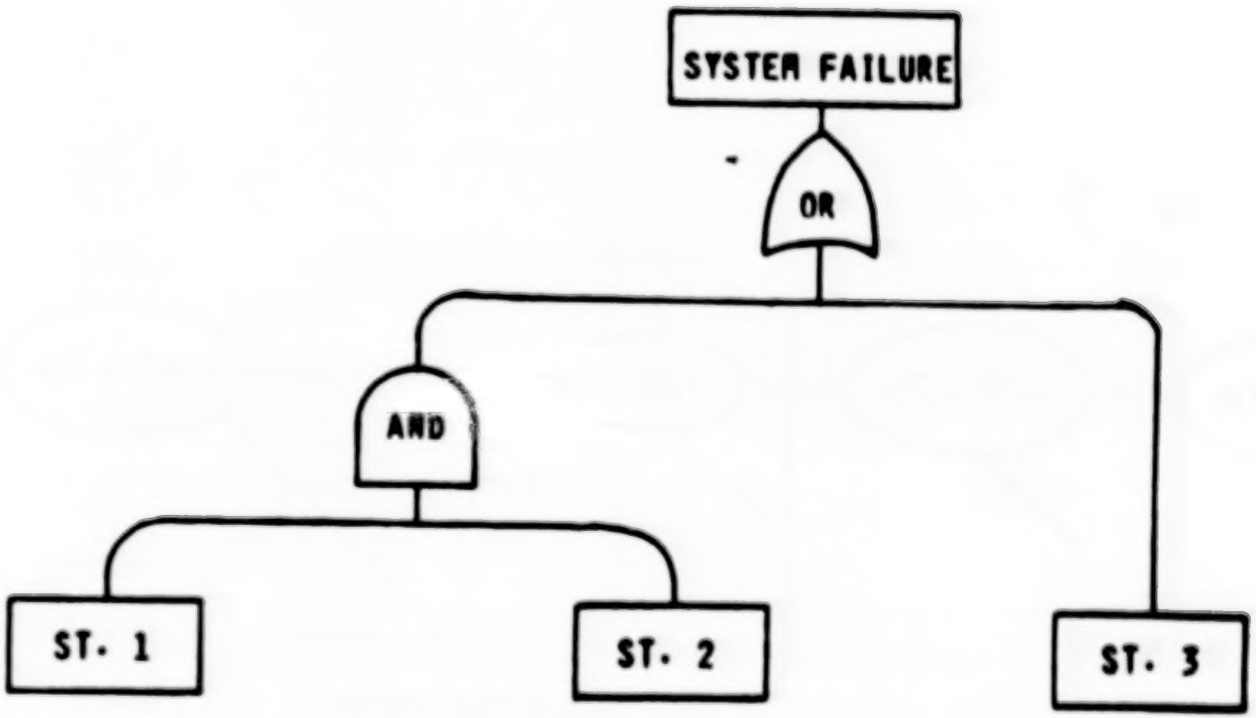
- STAGE: IDENTICAL MODULES, SAME FUNCTION
  N : NUMBER OF MODULES
  M : MINIMUM NUMBER OF MODULES

STAGE FAILURE

FAILURES IN STAGE > N-M

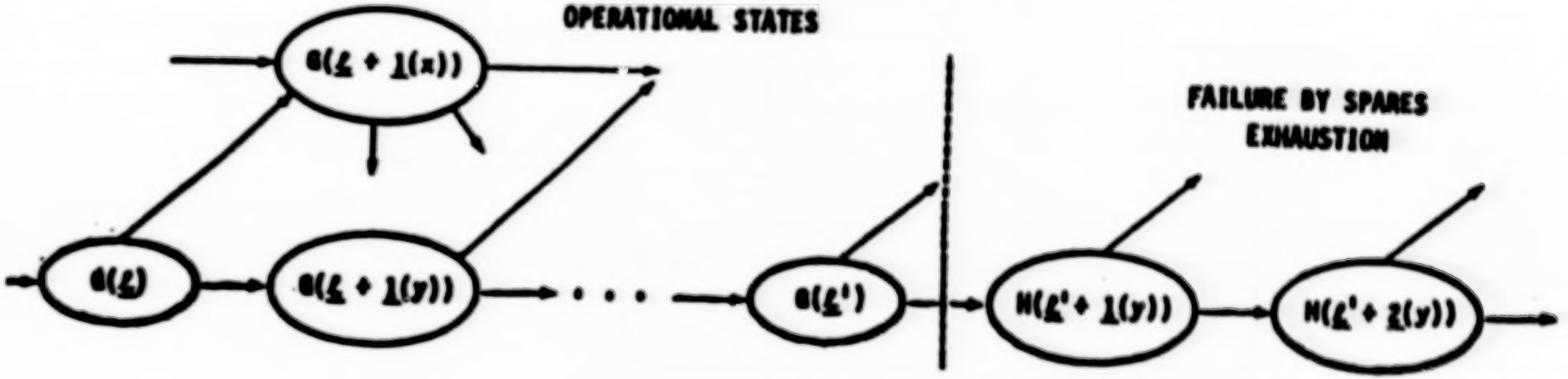
- SYSTEM FAILURE: MODULE EXHAUSTION
- SYSTEM LOGIC DEFINES MODULE EXHAUSTION

PARALLEL
SERIES
MIXTURE



STAGE FAILURES

CLASSICAL STOCHASTIC MODEL



$$\underline{\ell} = (\ell(1), \ell(2), \ldots, \ell(x), \ldots)$$

$\ell(x)$ = number of faulty stage-x modules

CLASSICAL MODEL : RELIABILITY

- $G(\underline{l})$ WITH PROB. $P(t|\underline{l})$

  $H(\underline{l})$ WITH PROB. $S(t|\underline{l})$

- $$1 - R(t) = \sum_{\underline{l} \in L} S(t|\underline{l})$$

- $P^{*}(t|\underline{l})$: PROBABILITY $\underline{l}$ FAULTS GIVEN PERFECT COVERAGE

  – BINOMIAL PROBABILITY –

- $$1 - R(t) = \sum_{\underline{l} \in L} P^{*}(t|\underline{l})$$

CARE III MODEL

- REDUNDANCY : N OUT OF N
- FAULT TOLERANCE WITH IMPERFECT FAULT-HANDLING

  ABILITY TO MASK FAULT (COVERAGE)
  UNTIL DETECTION, RECONFIGURATION

CLASSICAL AND CARE III MODELS

- MODULE: BASIC UNIT
  INDEPENDENT FAILURES

MODULE FAILURE OCCURRENCE RATE

$$\lambda(t) = \begin{cases} \lambda & \text{EXPONENTIAL} \\ \lambda\omega(\lambda t)^{\omega-1} & \text{WEIBULL} \end{cases}$$

- STAGE: IDENTICAL MODULES, SAME FUNCTION
  N : NUMBER OF MODULES
  M : MINIMUM NUMBER OF MODULES

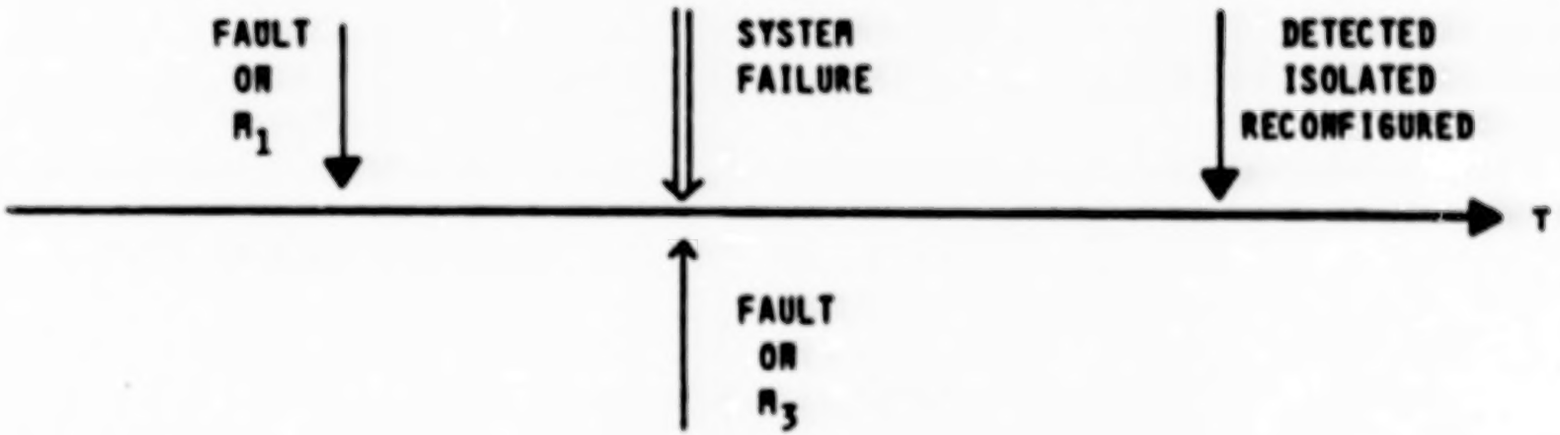
STAGE FAILURE

FAILURES IN STAGE > N-M

SYSTEM FAILURES

- EXHAUSTION : SYSTEM LOGIC
- IMPERFECT FAULT-HANDLING : DOMINANT MODE

SINGLE FAULT - VOTER
DOUBLE FAULT - 2 MODULES
IN A TRIAD
CRITICALLY COUPLED



ARCHITECTURE

- MODULE / STAGE

  N, M / SYSTEM TREE

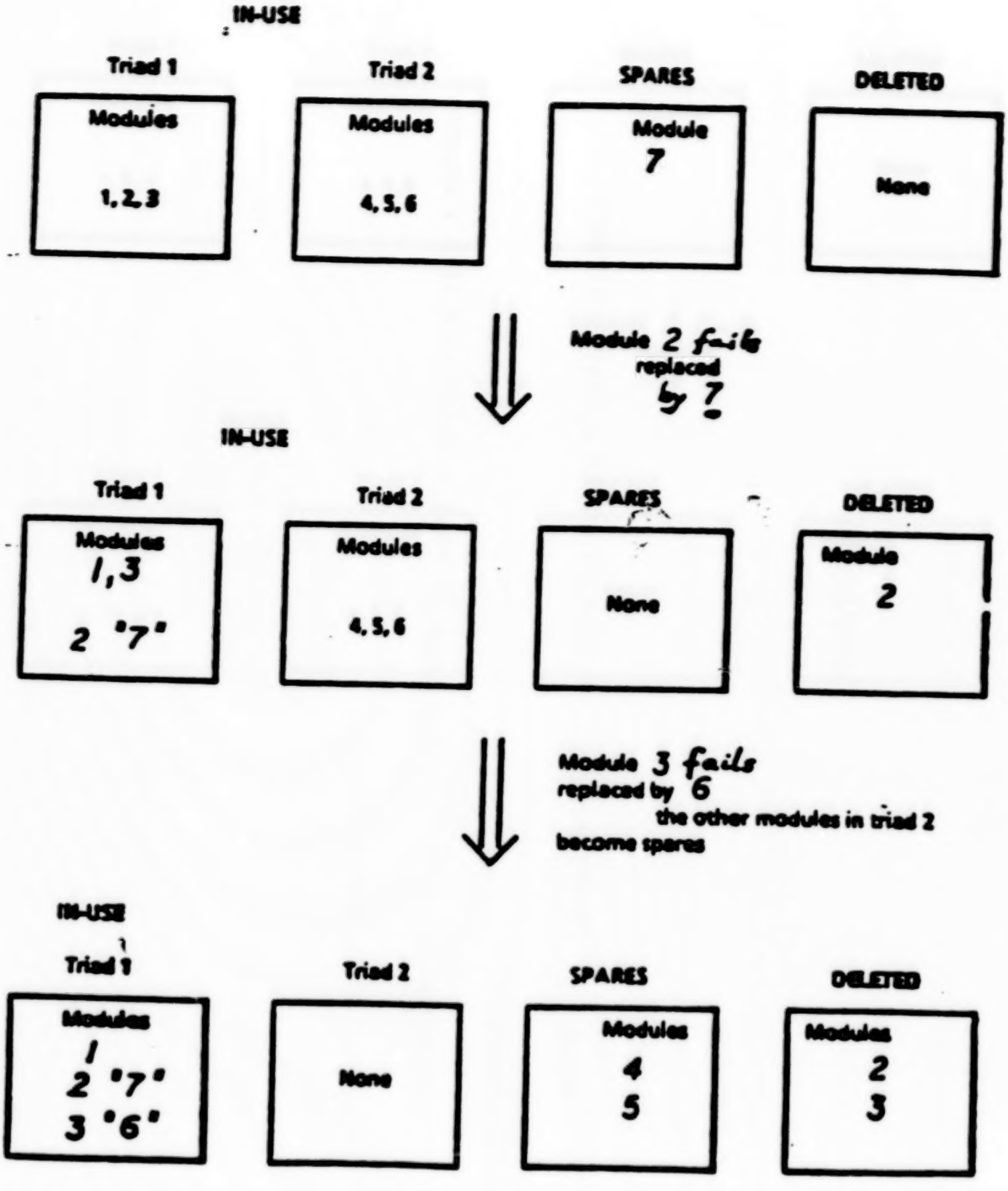
- MOP : NUMBER OF IN-USE MODULES SUBJECT TO CRITICAL PAIR FAILURES

- CRITICAL PAIRS

  PAIRS OF MODULES THAT MAY LEAD TO DOUBLE FAULT COVERAGE FAILURE

  FUNCTIONAL NUMBERING

ORIGINAL PAGE IS
OF POOR QUALITY



FAULTS

PER STAGE

SEVERAL TYPES
E.G. PERMANENT
INTERMITTENT
TRANSIENT

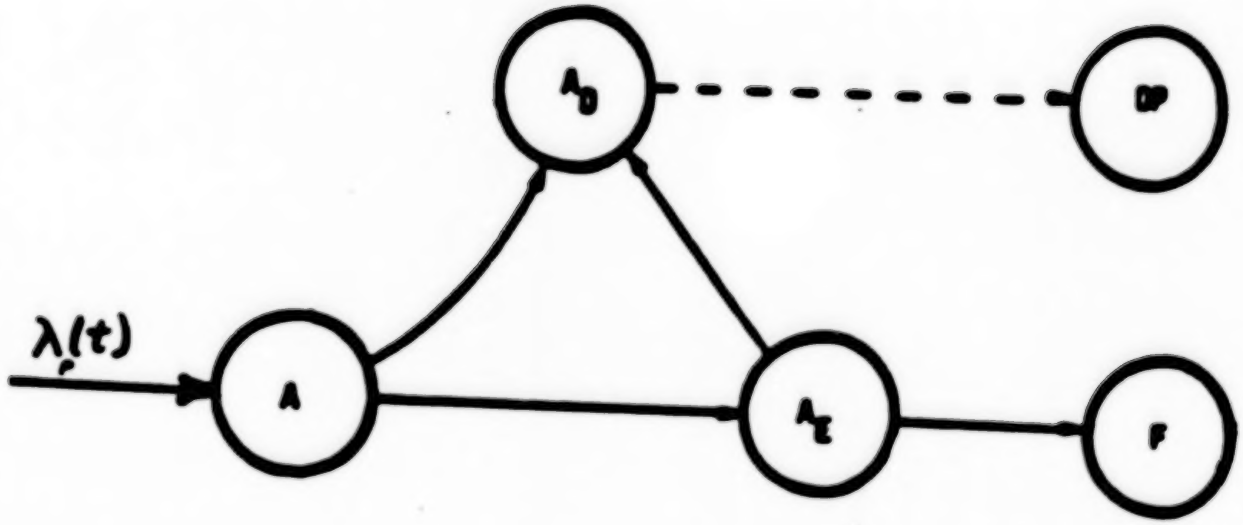
- OCCURRENCE RATE

$$\lambda(t) = \lambda\omega(t\lambda)^{\omega-1}$$

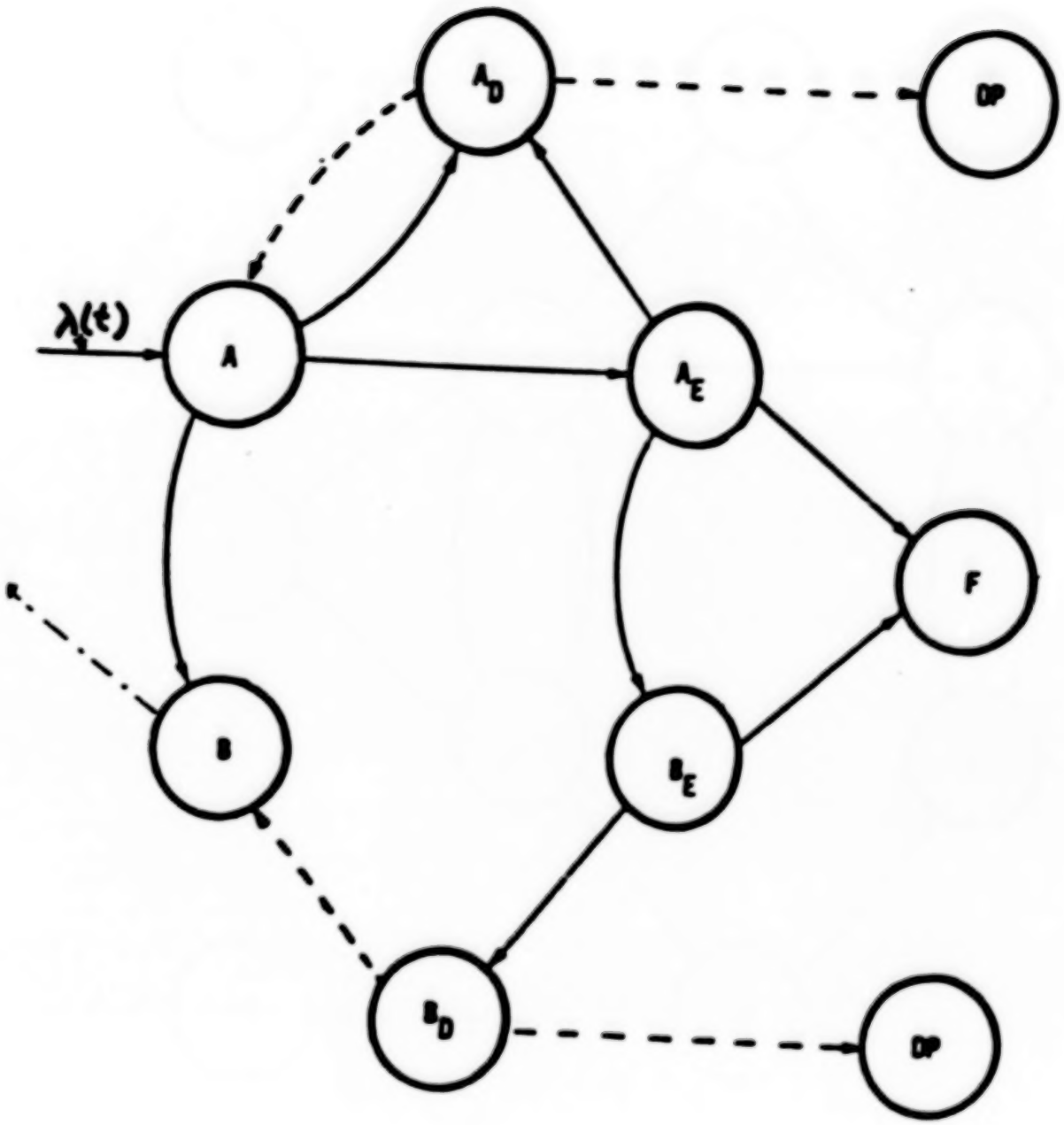
- HANDLING

COVERAGE MODEL : PERMANENT
INTERMITTENT
TRANSIENT

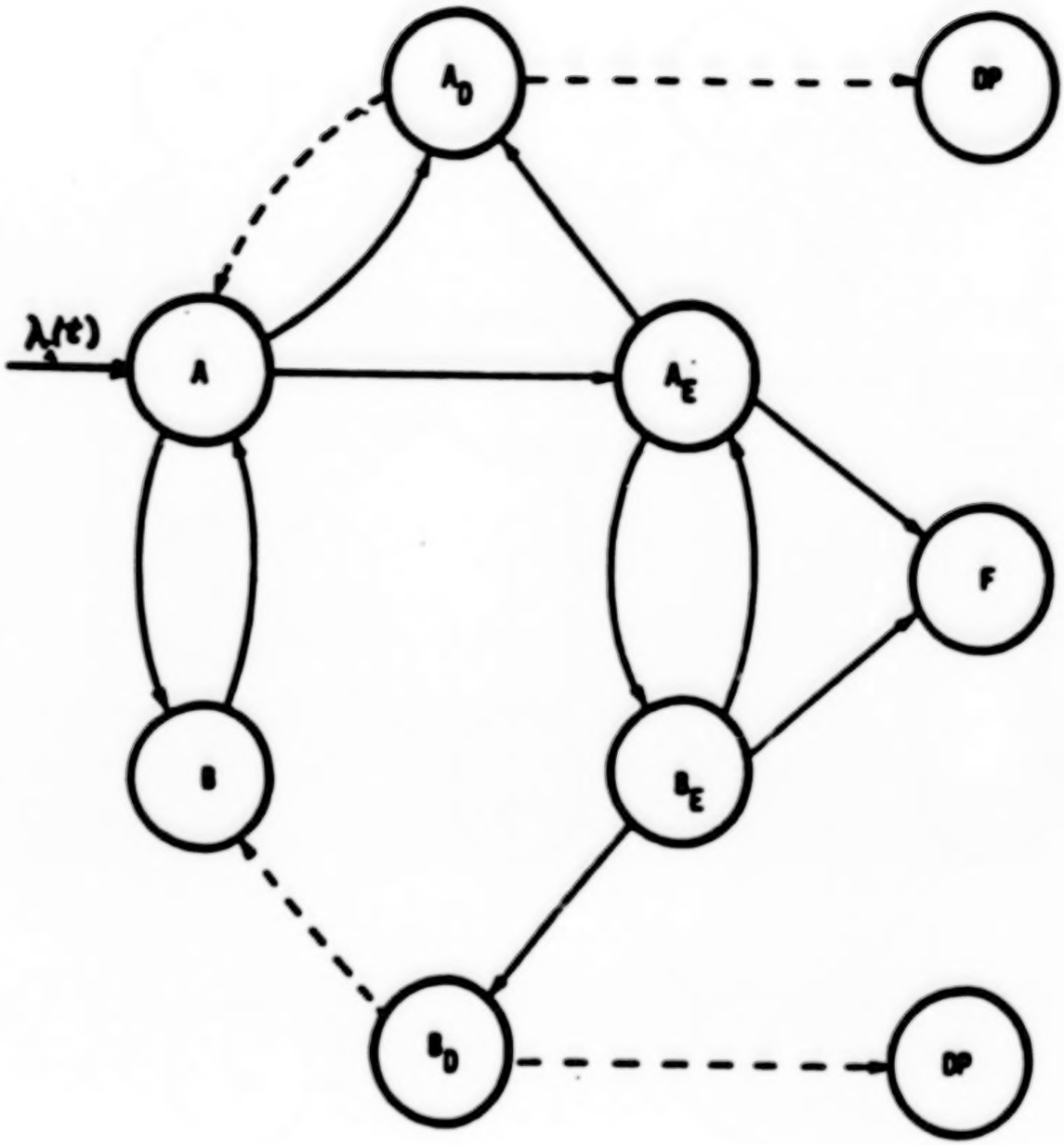
PERMANENT

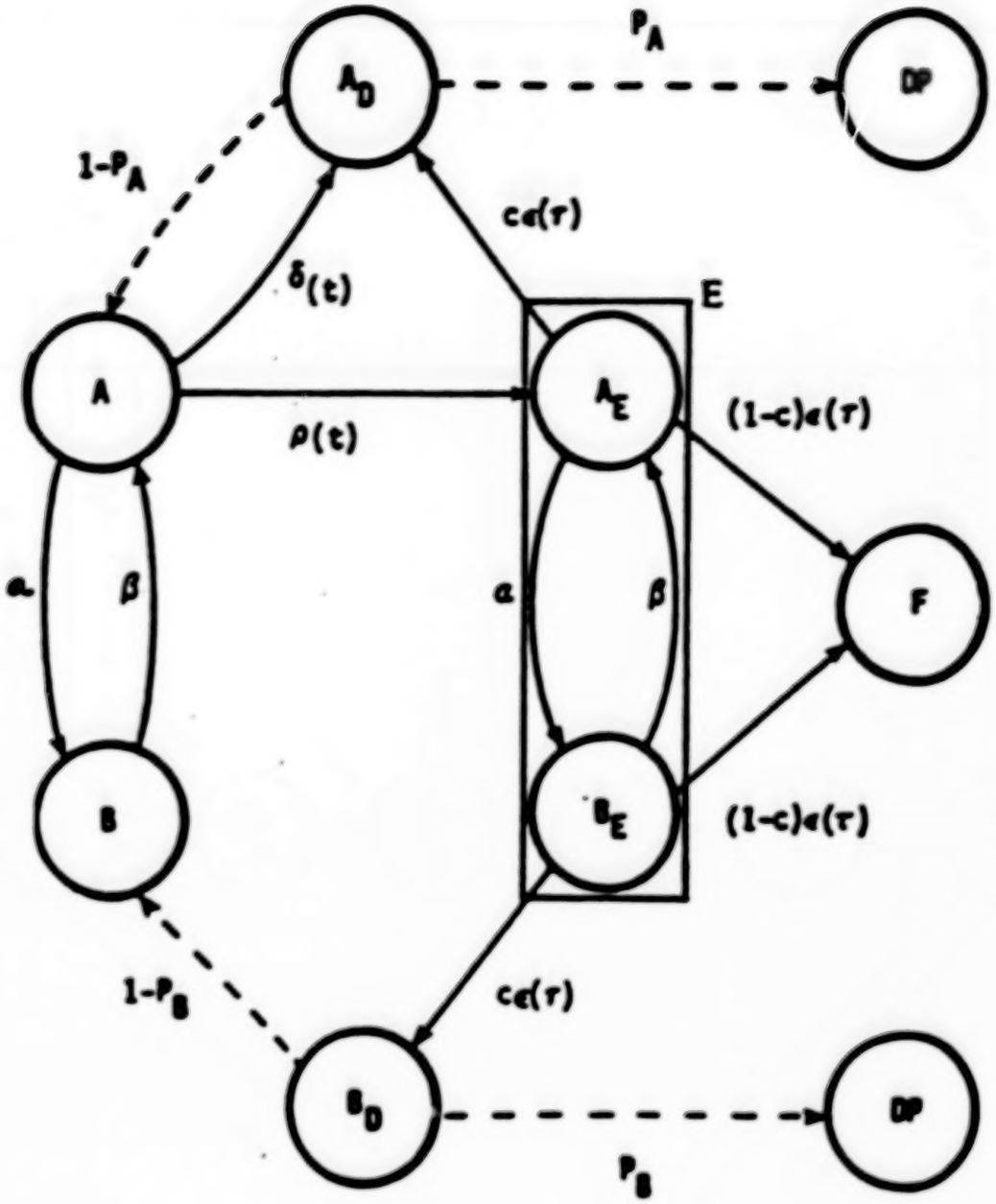


TRANSIENT



INTERMITTENT



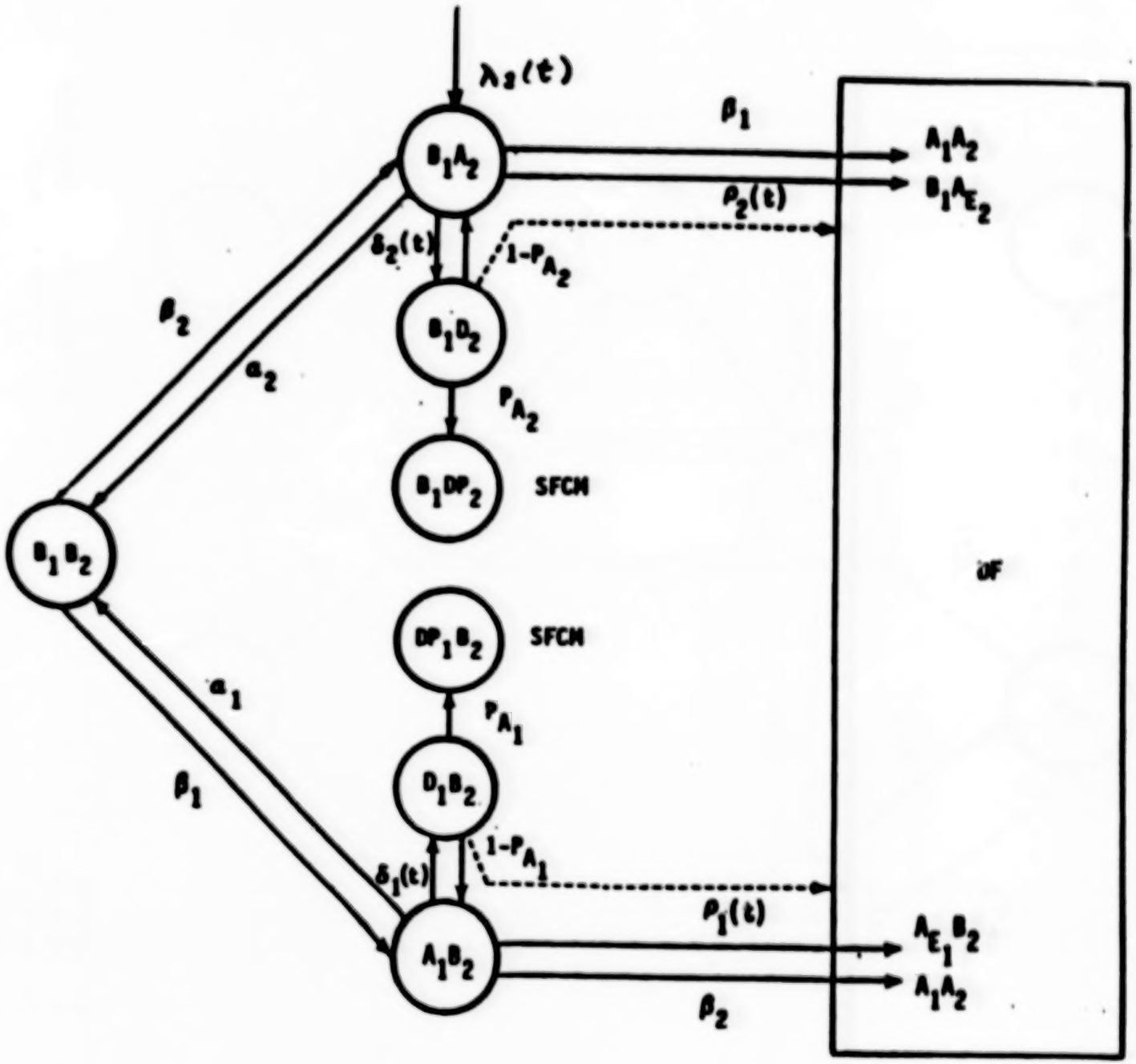


A: ACTIVE
B: BENIGN
D: DETECTED
E: ERROR
F: FAILURE
DP: DETECTED AS PERMANENT (NON-TRANSIENT)

t = time from entry into active state A

τ = time from entry into error state E

Single Fault Coverage Model


$\lambda_2(t)$
B_1A_2
β_1
A_1A_2
$B_1A_{E_2}$
$\rho_2(t)$
$\delta_2(t)$
$1-P_{A_2}$
B_1D_2
β_2
a_2
P_{A_2}
B_1DP_2
SFCM
B_1B_2
OF
DP_1B_2
SFCM
a_1
P_{A_1}
β_1
D_1B_2
$1-P_{A_1}$
$\delta_1(t)$
$\rho_1(t)$
$A_{E_1}B_2$
A_1B_2
A_1A_2
β_2

MICRO MODEL

- FAULT OCCURRENCE RATES
  - SINGLE FAULT MODEL
  - DOUBLE FAULT MODEL
  - CRITICAL PAIRS
  - SPARES
  - SYSTEM LOGIC
- OPERATIONAL/FAILURE STATES

  RELIABILITY ?
- SYSTEM OF INTEGRAL RENEWAL EQUATIONS
- FEASIBLE ?

SOLUTION

ULTRARELIABLE:

FAULT HANDLING

MUCH FASTER THAN

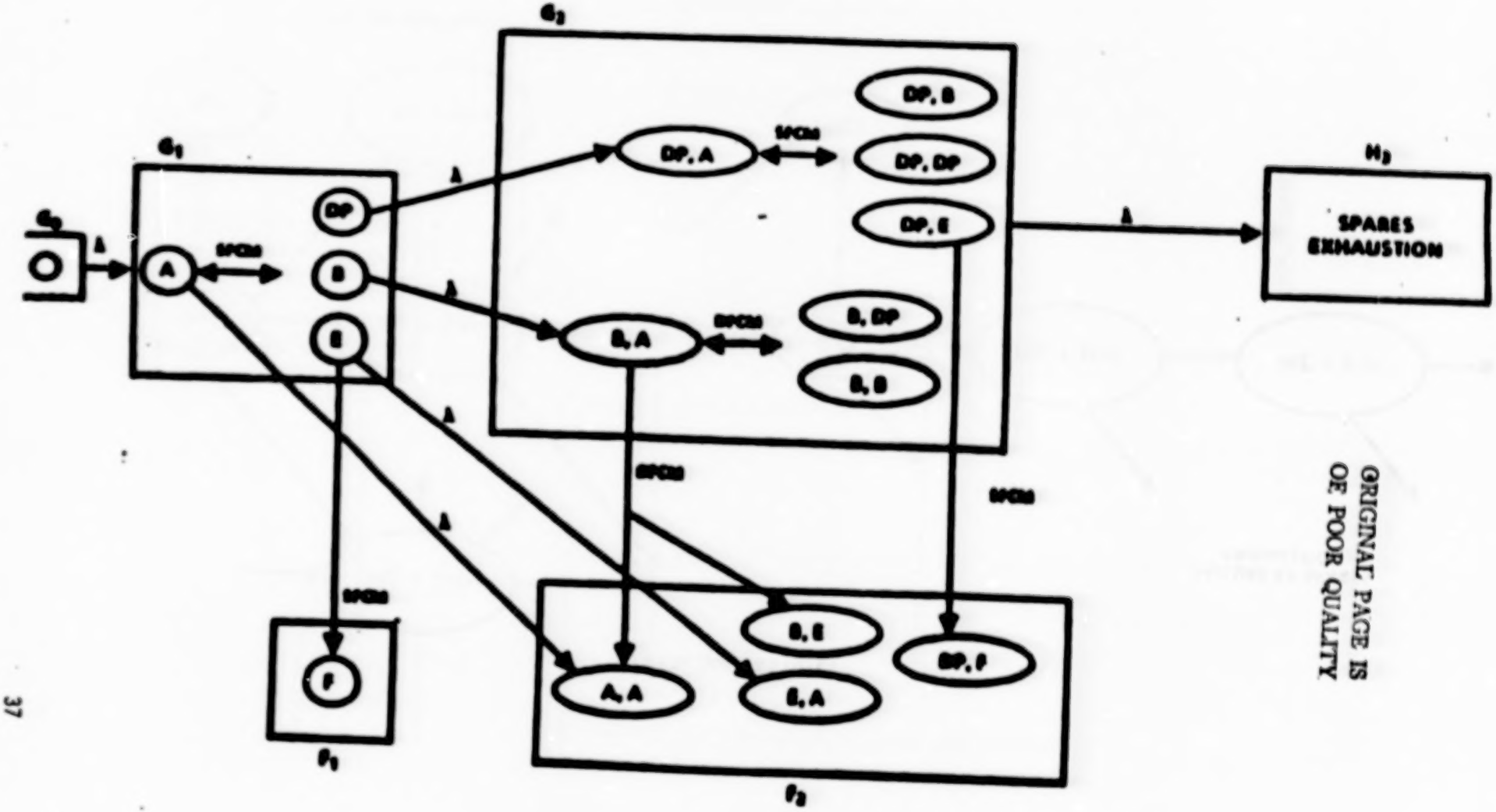
FAULT OCCURRENCE

MACRO MODEL

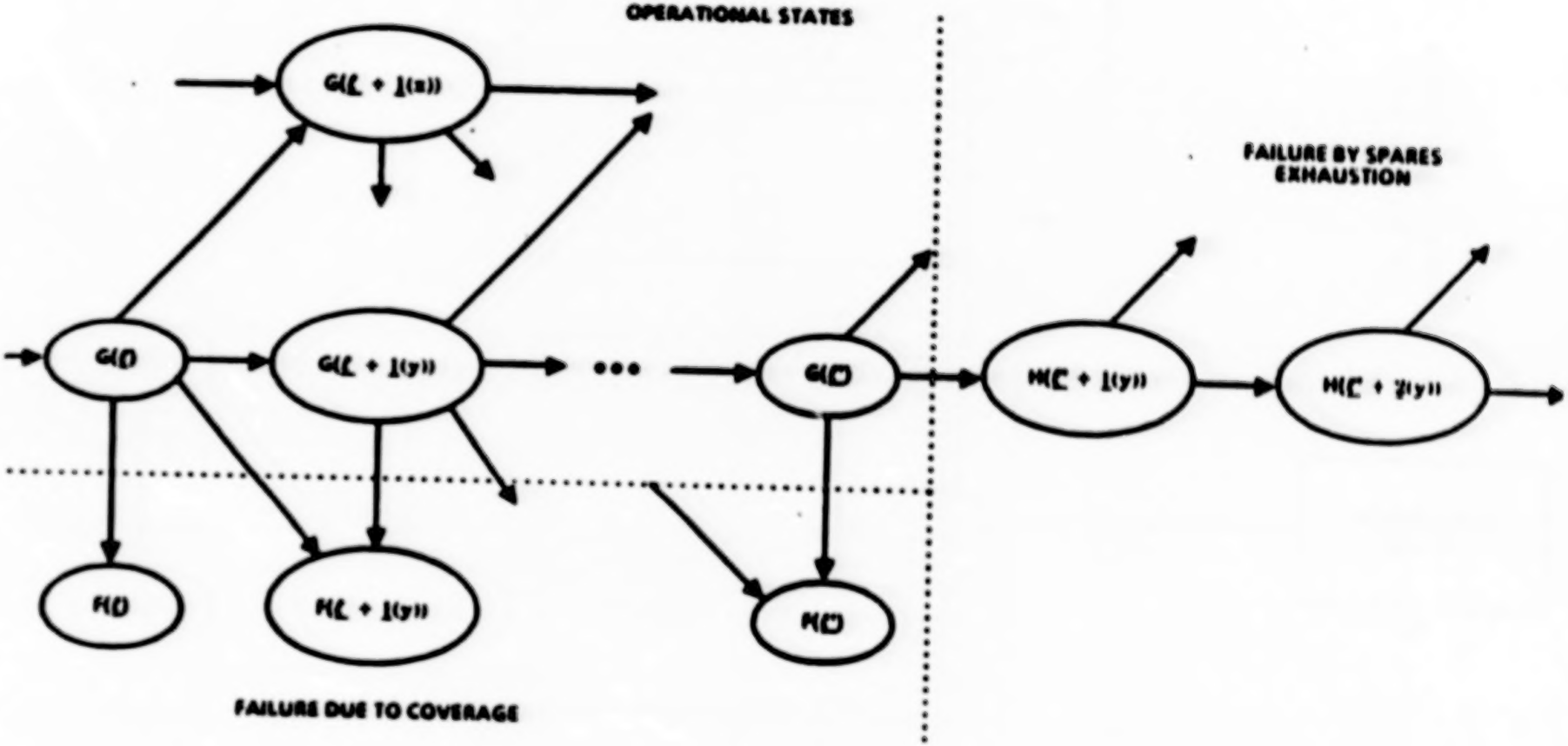
- o AGGREGATION
- o APPROXIMATE MARKOV PROCESS
- o DECOMPOSITION
  COVERAGE/RELIABILITY

EXAMPLE: TRIAD

PERMANENT /INTERMITTENT

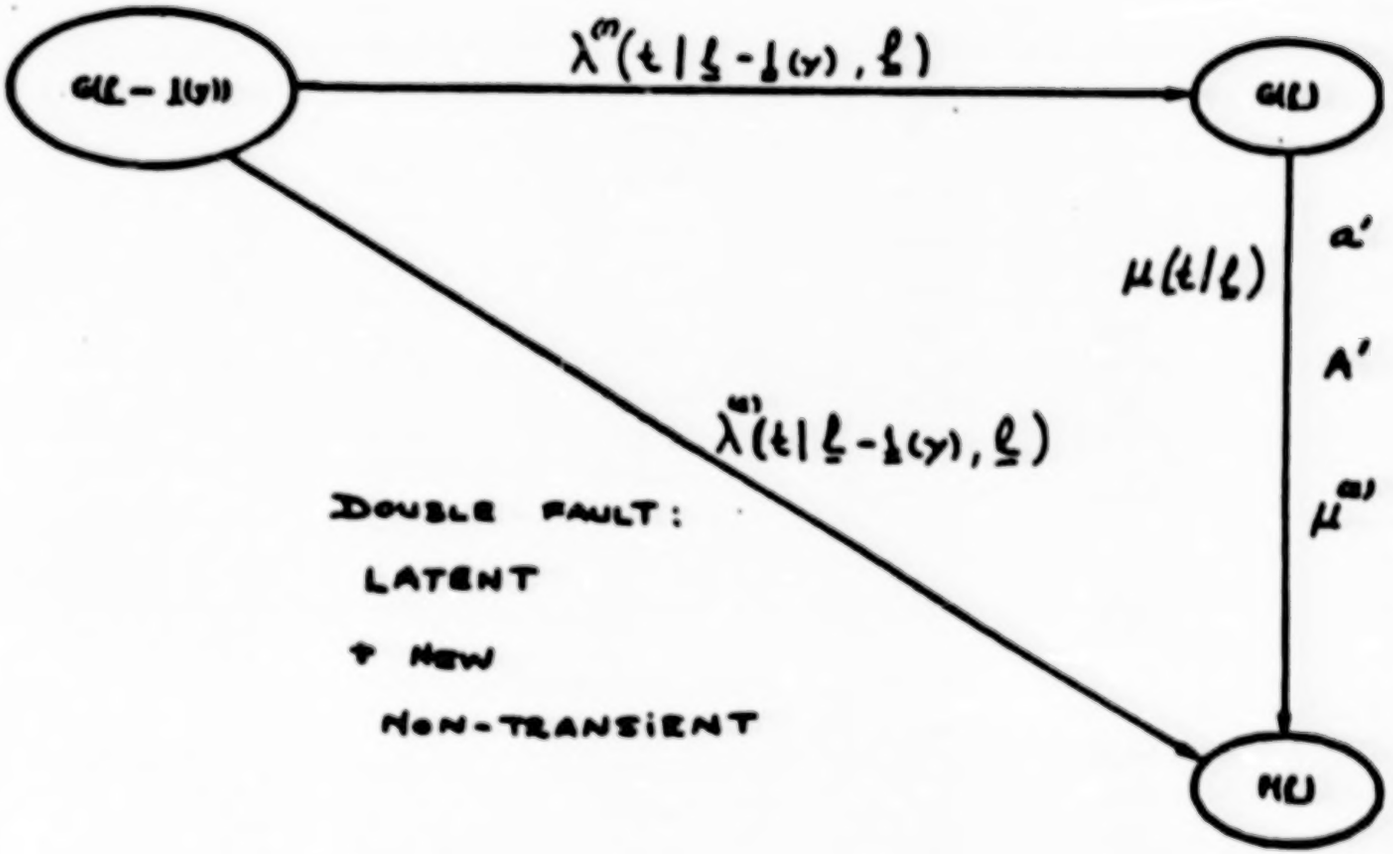


ORIGINAL PAGE IS
OF POOR QUALITY



General Structure of CARE III Aggregate Model

ORIGINAL PAGE IS
OF POOR QUALITY



DOUBLE FAULT:
LATENT
+ NEW
NON-TRANSIENT

a' : SINGLE

A' : DOUBLE LATENT

$\mu^{(a)}$: DOUBLE FAULT
LATENT +
NEW TRANSIENT

RELIABILITY

$$UR(t) = \sum_{\underline{\ell} \in L} Q(t|\underline{\ell}) + \sum_{\underline{\ell} \in \bar{L}} S(t|\underline{\ell})$$

$$S(t|\underline{\ell}) \leq P^{**}(t|\underline{\ell})$$

$$Q(t|\underline{\ell}) = \int_0^t K(\tau|\underline{\ell})\, d\tau$$

$$K(t|\underline{\ell}) \cong P^{**}(t|\underline{\ell})\, \mu(t|\underline{\ell}) +$$

$$+ \sum_{\nu} P^{*}(t|\underline{\ell} - \underline{1}(\nu))\ \lambda^{(\nu)}(t|\underline{\ell} - \underline{1}(\nu), \underline{\ell})$$

RTI'S USE OF CARE III

October 6, 1987

Charlotte O. Scheper

Research Triangle Institute

OUTLINE

- Comparative study of CARE III and ARIES 82
  - Objective
  - Technical approach
  - CARE III assessment
  - ARIES 82 assessment

- Comparison of on chip versus off chip redundancy

- Integration of performance and reliability tools

RTI

COMPARATIVE STUDY OF CARE III & ARIES 82

OBJECTIVES

- Determine suitability for AIPS analysis
- Compare CARE III and ARIES 82

RTI

TECHNICAL APPROACH

- Obtain and review AIPS architecture information
  - Objectives and requirements
  - Features and building blocks
  - Impact on reliability assessment
- Overview of CARE III and ARIES
- Apply CARE III and ARIES to problems
  - Problems selected to demonstrate relative strengths and weaknesses
  - Problems selected so that solution could be obtained by standard analysis techniques based on Markov model

RTI

CARE III ASSESSMENT
OUTSTANDING FEATURES

- Can handle large systems
- Flexible fault handling model
- Can have non-constant fault occurrence rates
- Well tested and verified

RTI

CARE III ASSESSMENT
APPLICABLE SYSTEM CHARACTERISTICS

- Best suited for systems where:
  - The mission time is short relative to the time between failure occurrences
  - The fault recovery time is short relative to the time between failure occurrences
  - Either the network reliability cannot impact system reliability or the network can be treated as an independent subsystem whose reliability can be determined by other means
  - Near coincident multiple faults of order greater than two are not relevant
  - System reliability should be in the extremely to ultrareliable regime

RTI

CARE III ASSESSMENT
POTENTIAL LIMITATIONS

- The fundamental assumption that sojourn times in the fault handling model are small relative to the time between fault occurrences may not be valid for latent faults or for some intermittent faults

- The fault handling models used are independent of system state

- The fault handling model is constrained
  - To a single entry state
  - To have identical transition rates (α , β) between active and benign for faulted and error-producing states
  - Transitions between some states of the model are omitted

- The double fault model is conservative
  - A system failure results if two critically coupled faults occur even though neither has produced an error

RTI

ARIES ASSESSMENT
OUTSTANDING FEATURES

- The capability to model closed or open systems
- Spare modules can have failure rates that are different than active module failure rates
- A state transition matrix can be used to describe a system
- An interactive user interface

RTI

ARIES ASSESSMENT
POTENTIAL LIMITATIONS

- Instantaneous coverage may not be adequate for modeling some systems
- Constant failure rates are not adequate for modeling certain components of aerospace systems
- System sizes are limited to relatively small systems
- The accuracy of the results are suspect for highly reliable systems
- The eigenvalues of the state transition matrix must be distinct

RTI

INTEGRATION OF PERFORMANCE AND RELIABILITY TOOLS

PURPOSE

To develop an integrated set of tools to assist the system architect in the design of high-performance, highly reliable systems.

RTI

TOOL DEVELOPMENT GOALS

- Tools for building an interrelated description of the system and its mission
  - Mission scenarios
  - System software
  - System hardware
- Tools for making tradeoffs between different system requirements
  - System throughput
  - System response time
  - System reliability
- Tools for maintaining consistent models of the system
  - Reliability models
  - Hardware models
  - Software models
  - Fault models

RTI

PHASE I

- Build paradigm model
- Analyze paradigm model
- Define methodology

RTI

PHASE II

- Use methodology to revise the paradigm
- Specify tools to support the methodology
- Find existing tools which support the methodology

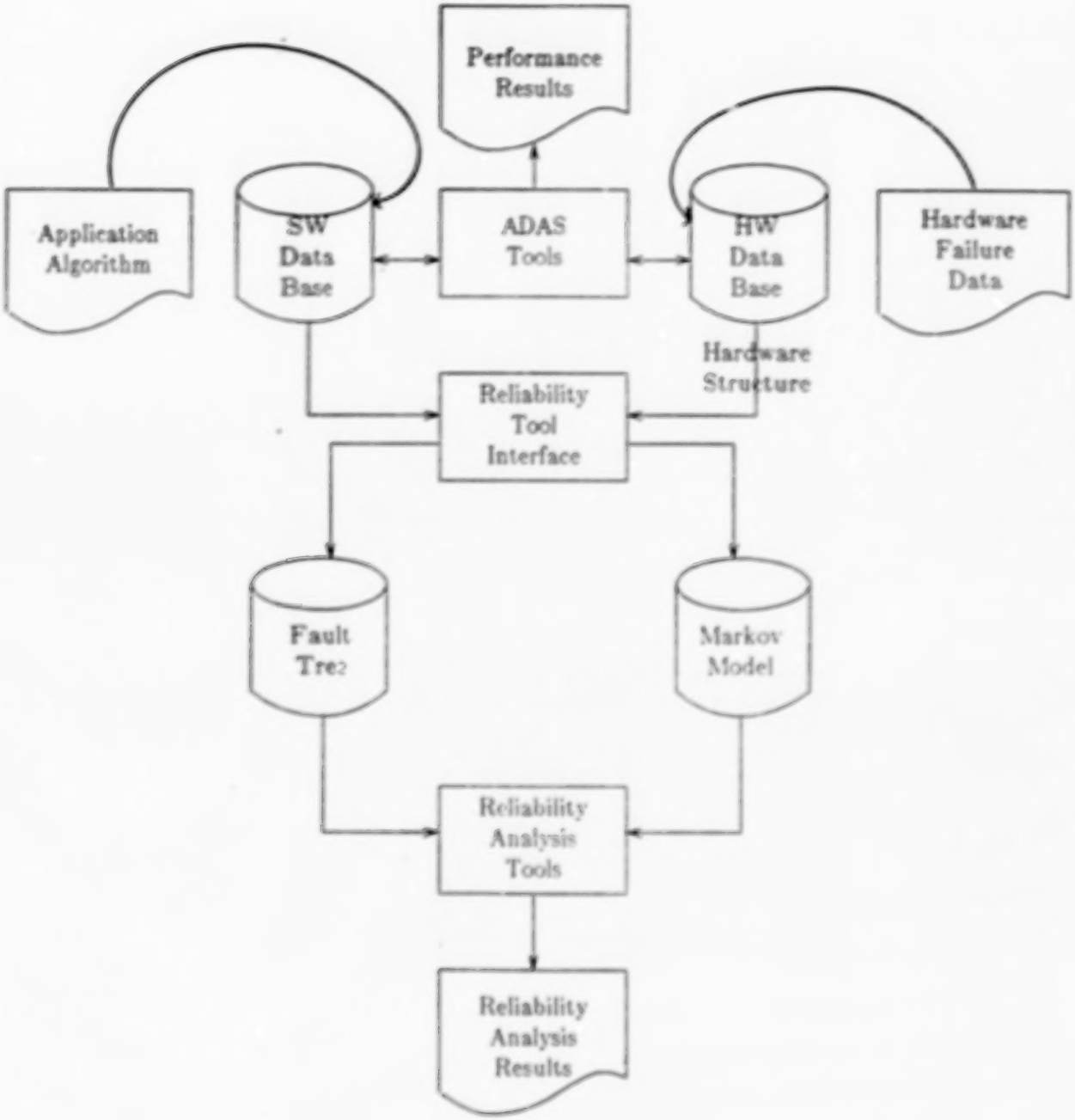
RTI

PHASE III

- Design interfaces between existing tools
- Build and test interfaces between tools
- Beta test the integrated tool sets
- Demonstrate integrated tool sets

RTI

POSSIBLE INTERFACE BETWEEN ADAS AND RELIABILITY ANALYSIS TOOLS



SUMMARY

- Areas of applicability
- Role in integrated tools

USE OF CARE III FOR FLIGHT CONTROLS DEVELOPMENT AT NORTHROP

October 6, 1987

Jack Flynn

Northrop Corporation

OVERVIEW

- NORTHROP FLIGHT CONTROLS DEVELOPMENT
- CAREIII EXPERIENCE
- CAREIII ENHANCEMENTS
- IBM INSTALLATION DETAILS
- SUMMARY

NORTHROP FLIGHT CONTROLS DEVELOPMENT

- PRELIMINARY TRADES OF FLIGHT CONTROL SYSTEMS
  - DUAL, TRIPLEX, AND QUAD ARCHITECTURES
  - MANNED AND UNMANNED VEHICLES
- CAREIII USED FOR INITIAL SAFETY AND MISSION PROBABILITY CALCULATIONS SINCE 1985
- USE FAULT TREE FEATURES MORE THAN FAULT HANDLING FEATURES
- OFTEN BUILD SPECIFIC DETAILED FORTRAN RELIABILITY MODEL FOR FINAL CANDIDATE

ORIGINAL PAGE IS
OF POOR QUALITY

CARE III EXPERIENCE

- USEFUL TOOL
  - REASONABLE SETUP AND MODIFICATION
  - SYNTAX CHECKS ARE USEFUL FOR EARLY ERROR DETECTION
- DEPENDENCY MODELLING QUICKLY REACHES STAGE LIMITS AND UNACCEPTABLE RUN TIMES
- IBM HOST LACKS USER FRIENDLY INTERFACE

ORIGINAL PAGE IS
OF POOR QUALITY

CARE III ENHANCEMENTS

- DEVELOPED
  - GRAPHICS POST PROCESSORS (DISSPLA AND GDDM)
    - EASY COMPARISON BETWEEN CONFIGURATIONS
    - SYSTEM ENGINEER/ANALYST INTERFACE
- DESIRED
  - DIRECT GRAPHICAL DEFINITION
  - P* SUMMARY FOR INDIVIDUAL STATE VECTORS
  - VECTORIZABLE FORTRAN CODE

ORIGINAL PAGE IS
OF POOR QUALITY

IBM INSTALLATION DETAILS

- ERROR STOP'S CHANGED TO STOP 12'S TO PASS CONDITION CODES BETWEEN CATALOGED PROCEDURE STEPS

- OUTPUT FORMAT CHANGED TO FIT RESULTS ON AN 80 CHARACTER TERMINAL

- MAXPRT INCREASED FROM 11 TO 13 BECAUSE SIGNIFICANT TERMS WERE BEING IGNORED

- DEVELOPED PREPROCESSOR TO STRIP LINE NUMBERS BEFORE CAREIN
  - LINE NUMBERS INTERFERE WITH IBM NAMELIST INPUT
  - LINE NUMBERS USED BY IBM SPF TO TRACK CHANGED LINES

- CINAME - RELEASE VER. 2.0; DEVEL. VER. 4, REV 3

- COVRGE, CARE3 - RELEASE VER. 1.0; DEVEL. VER. 4, REV 3

- INSTALLED ON 3090, 3081, 4341 MACHINES

SUMMARY

- CAREIII IS USEFUL TOOL FOR PRELIMINARY EVALUATION OF FLIGHT CONTROL SYSTEM SAFETY OF FLIGHT AND MISSION ABORT PROBABILITY CALCULATIONS

- DESIRE TO HAVE DIRECT GRAPHICAL INPUT OF FAULT TREE DEFINITION

CARE III MODEL

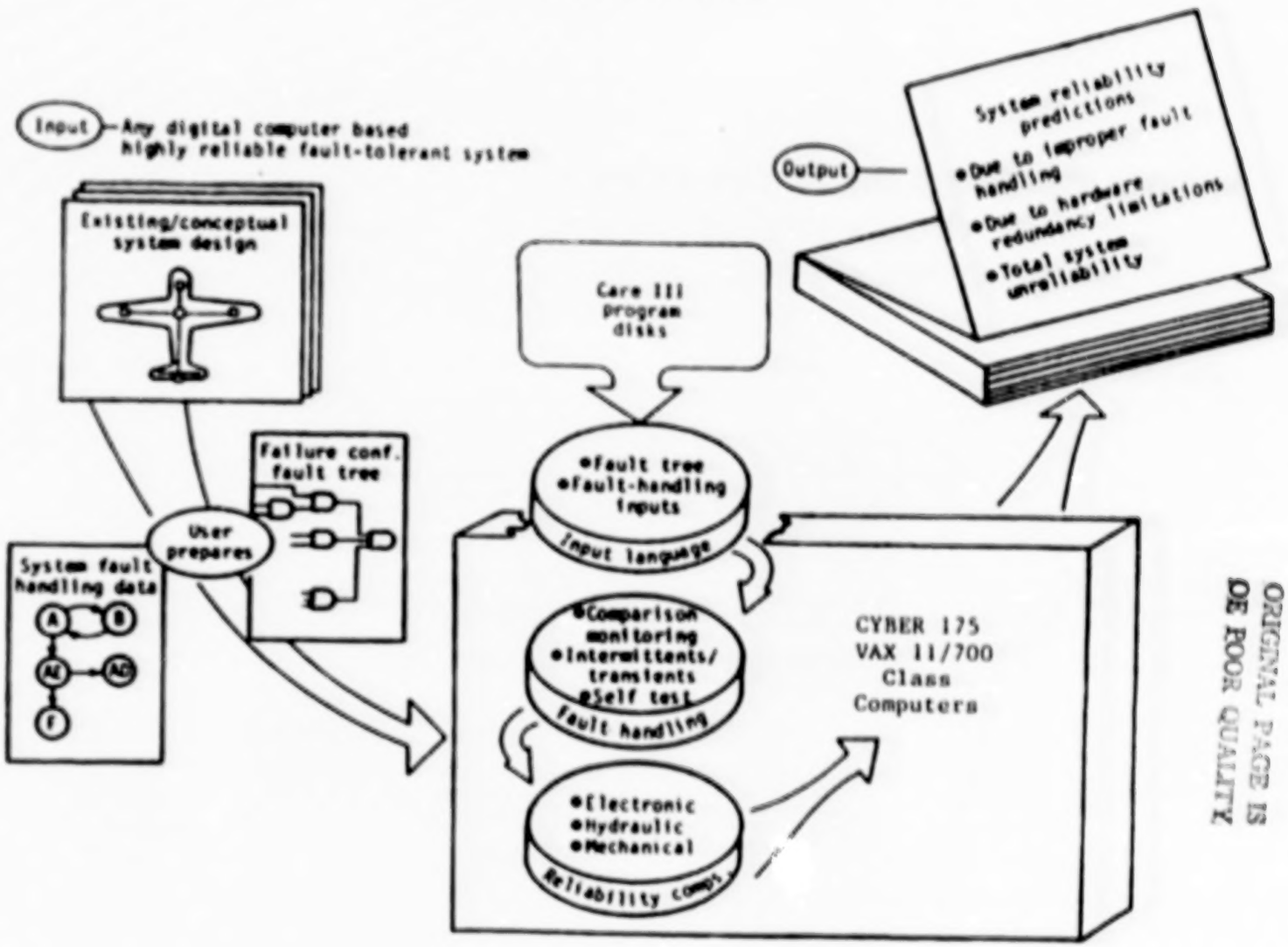
USER'S OVERVIEW

October 7, 1987

John Sight

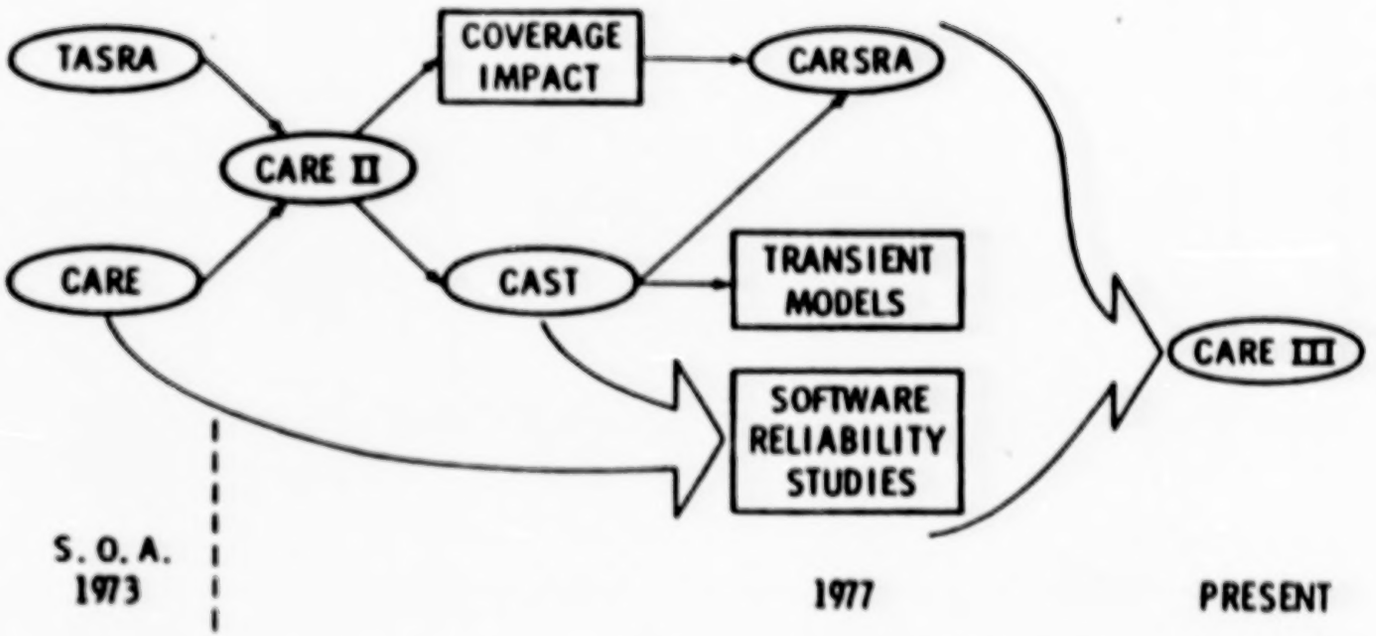
Northrop Corporation

CARE III USER PROCESS



ORIGINAL PAGE IS
OF POOR QUALITY

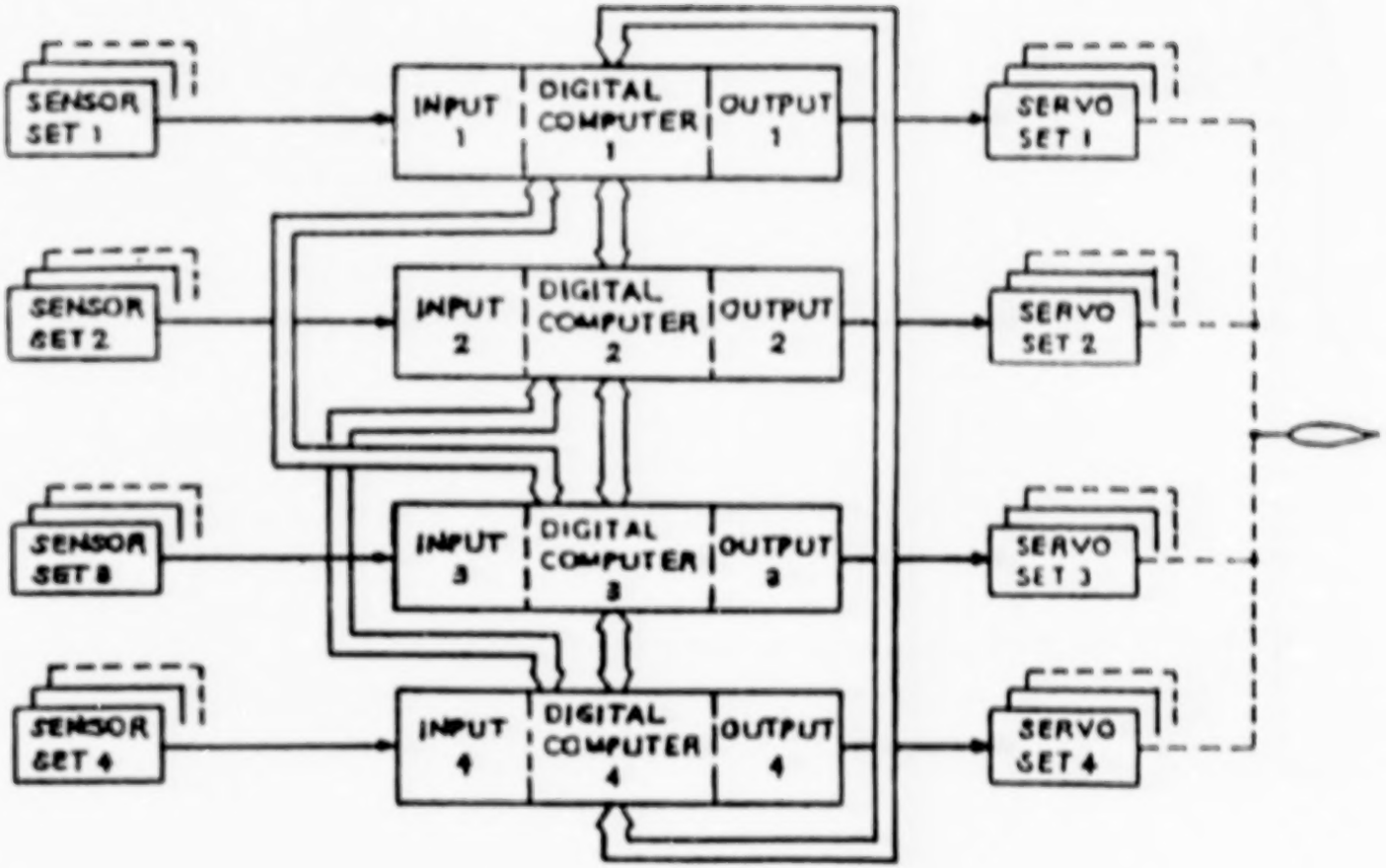
CARE III EVOLUTION



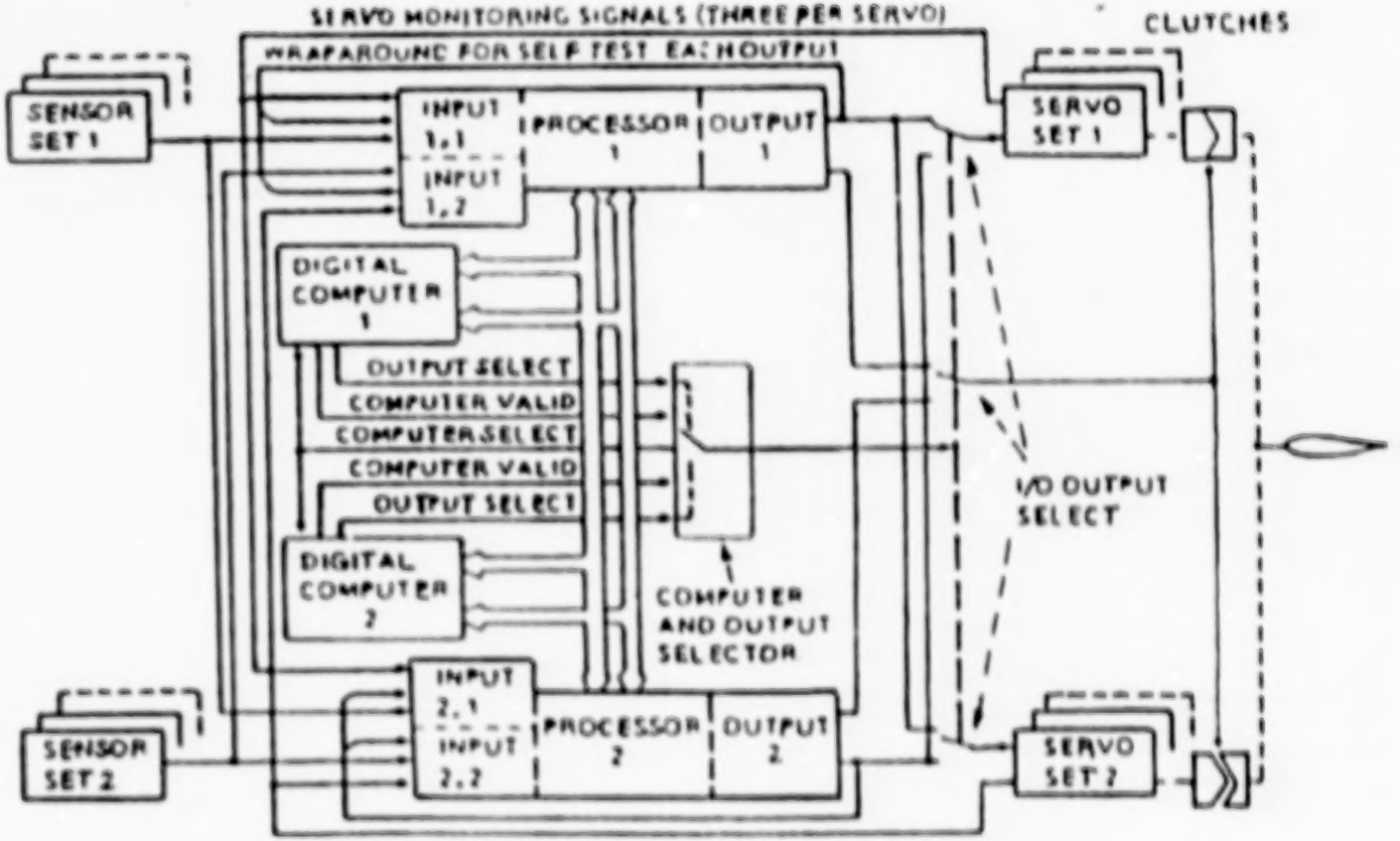
FLIGHT CONTROL COMPUTER ASSESSMENT

- FLIGHT CONTROL SYSTEM ASSESSMENT
- TRANSIENT-FAULT MODELING
- SOFTWARE-ERROR AND REDUNDANCY MODELING

QUADRUPLEX VOTED SYSTEM



DUPLEX SYSTEM WITH IN-LINE SELF-MONITORING



ORIGINAL PAGE IS
OF POOR QUALITY

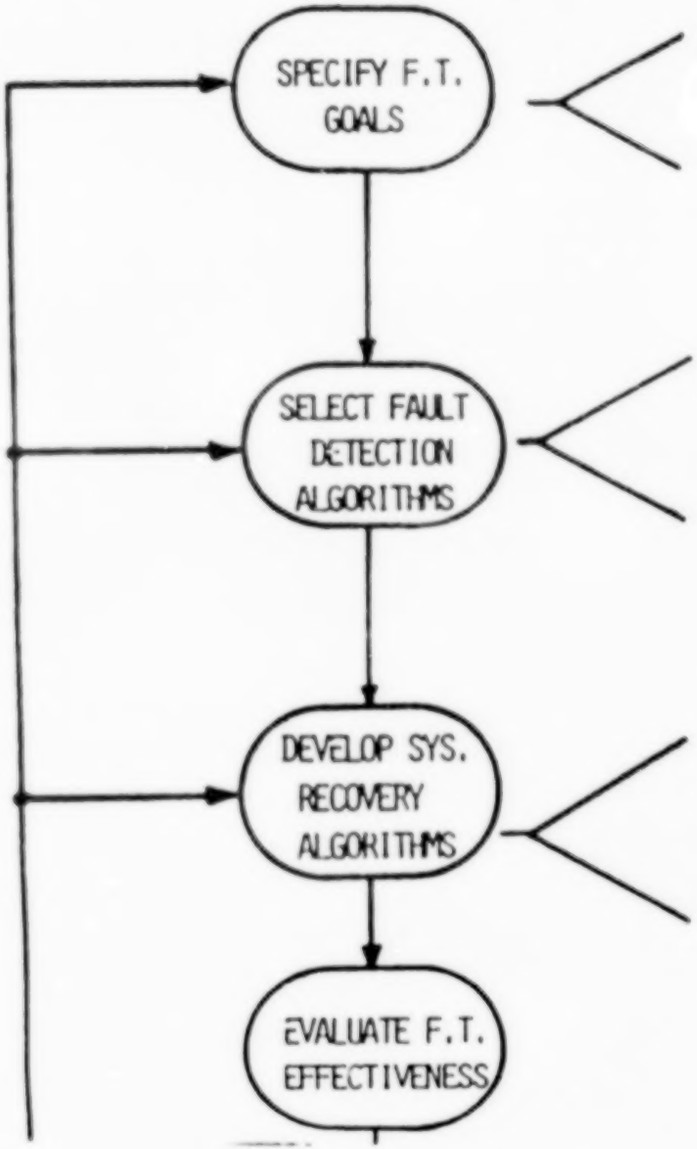
AREAS ADDRESSED BY ANALYTIC MODELLING

- EXHAUSTION OF HARDWARE RESOURCES
- IMPERFECT FAULT DETECTION, ISOLATION, AND RECONFIGURATION

AREAS NOT ADDRESSED BY ANALYTIC MODELLING

- DESIGN ERRORS
- INDUCED FAILURE

FAULT-TOLERANT DESIGN PROCESS



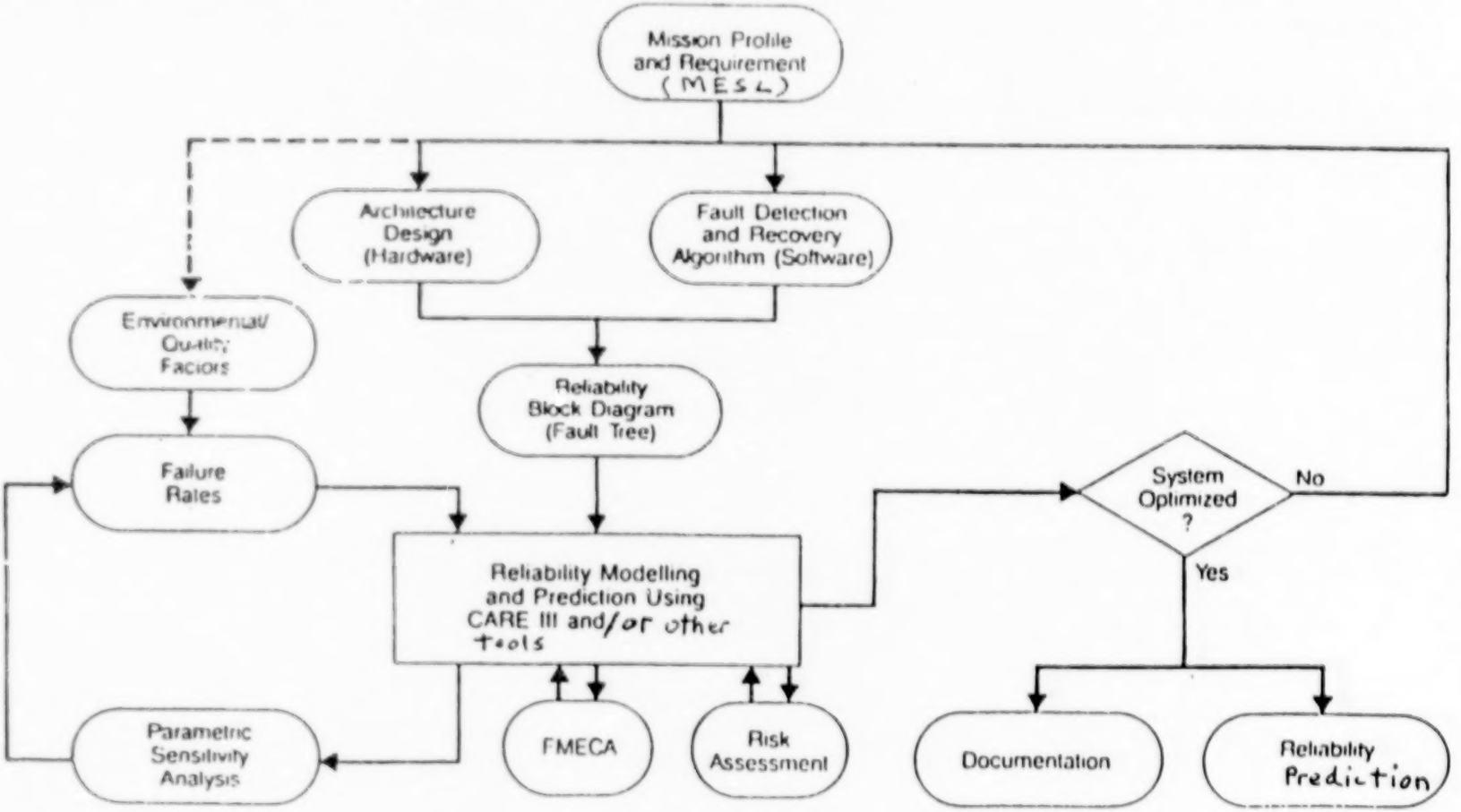
- IDENTIFY CLASSES OF FAULTS TO BE TOLERATED
- SET QUANTITATIVE GOALS OF RELIABLE OPERATION
- POSTULATE EVALUATION METHODS TO BE APPLIED

- CROSS-CHANNEL COMPARISON
- ERROR DETECTION & ERROR CORRECTION CODES
- IN-LINE SELF-MONITORING

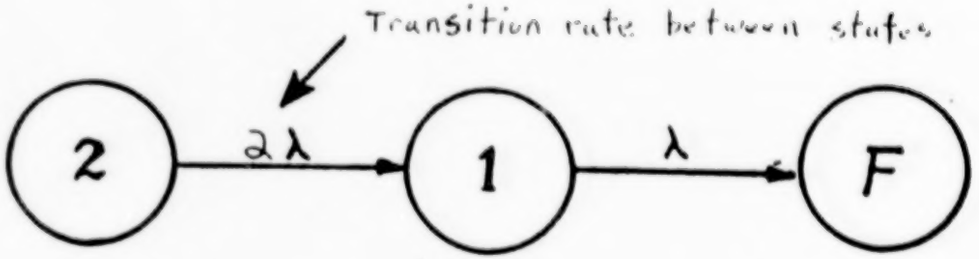
- TRANSIENT FAULT RECOVERY
- RECOVERY TO ORIGINAL PERFORMANCE
- RECOVERY TO REDUCED PERFORMANCE
- SAFE SHUTDOWN
- FAULTS AND ENVIRONMENTAL FACTORS LOGGING

Reliability Analysis Approach and Methodology

Influence on Design



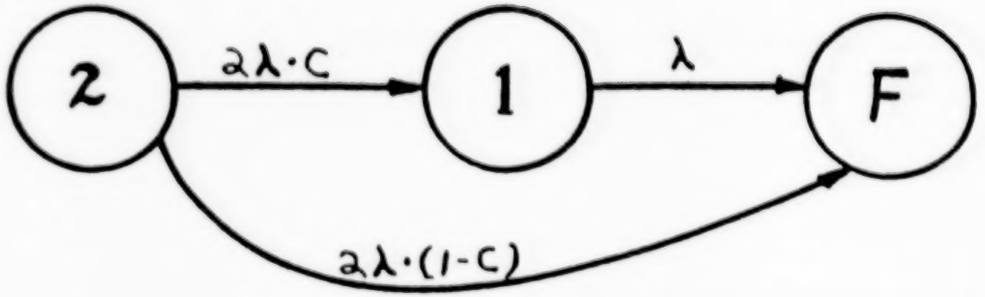
STATE DIAGRAMS OF A DUAL REDUNDANT SYSTEM



(A) PERFECT FAULT COVERAGE (C = 1.0)

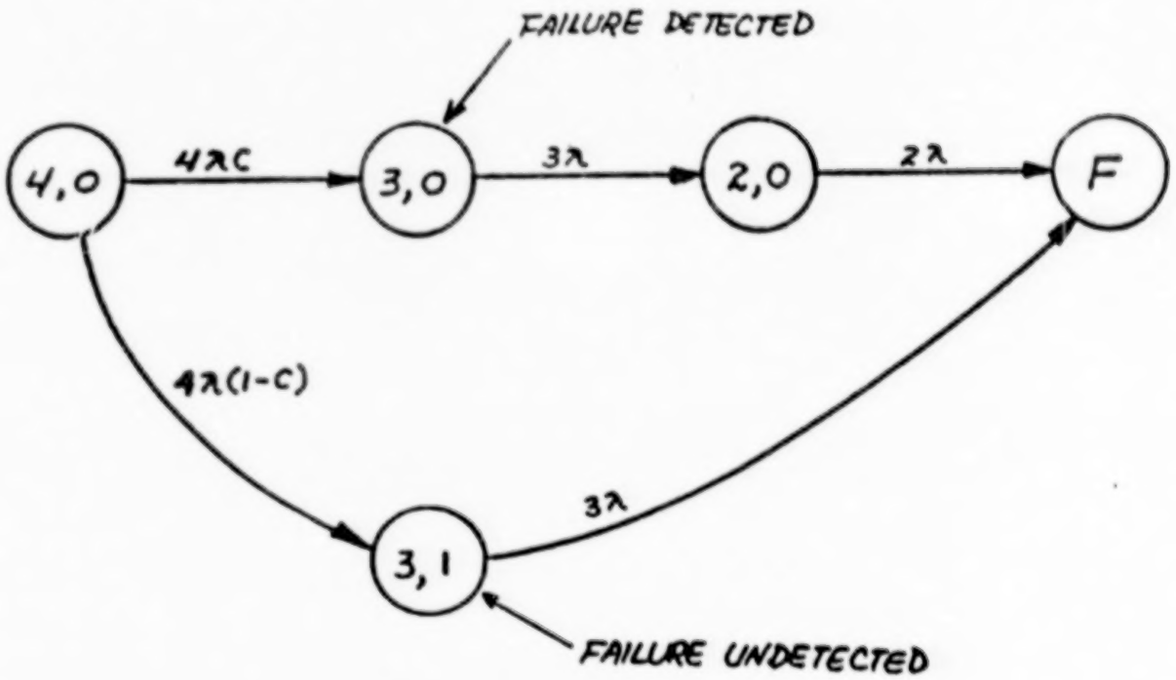
λ: component failure rate

C: fault coverage factor



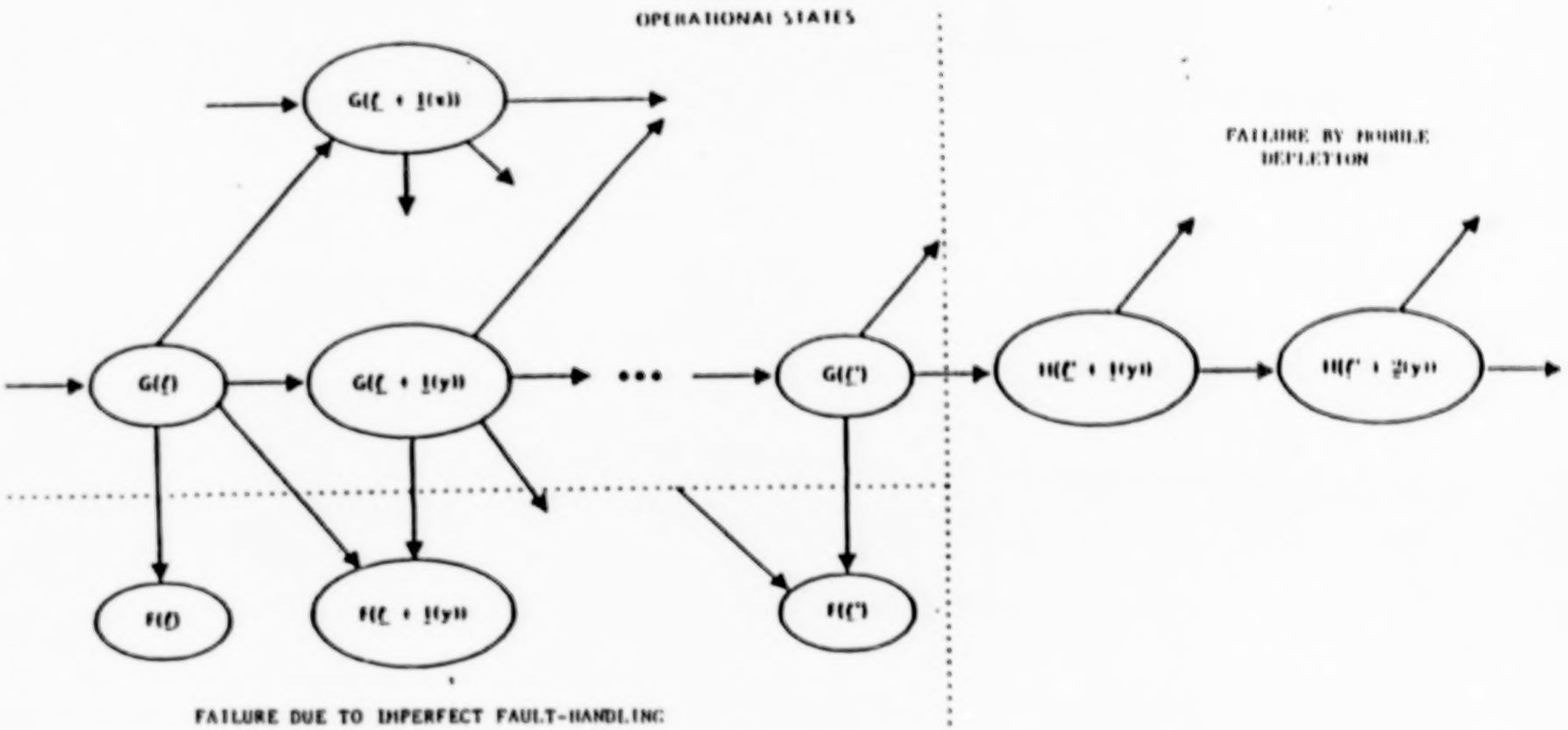
(B) IMPERFECT FAULT COVERAGE (C < 1.0)

STATE DIAGRAM OF A QUAD-REDUNDANT SYSTEM

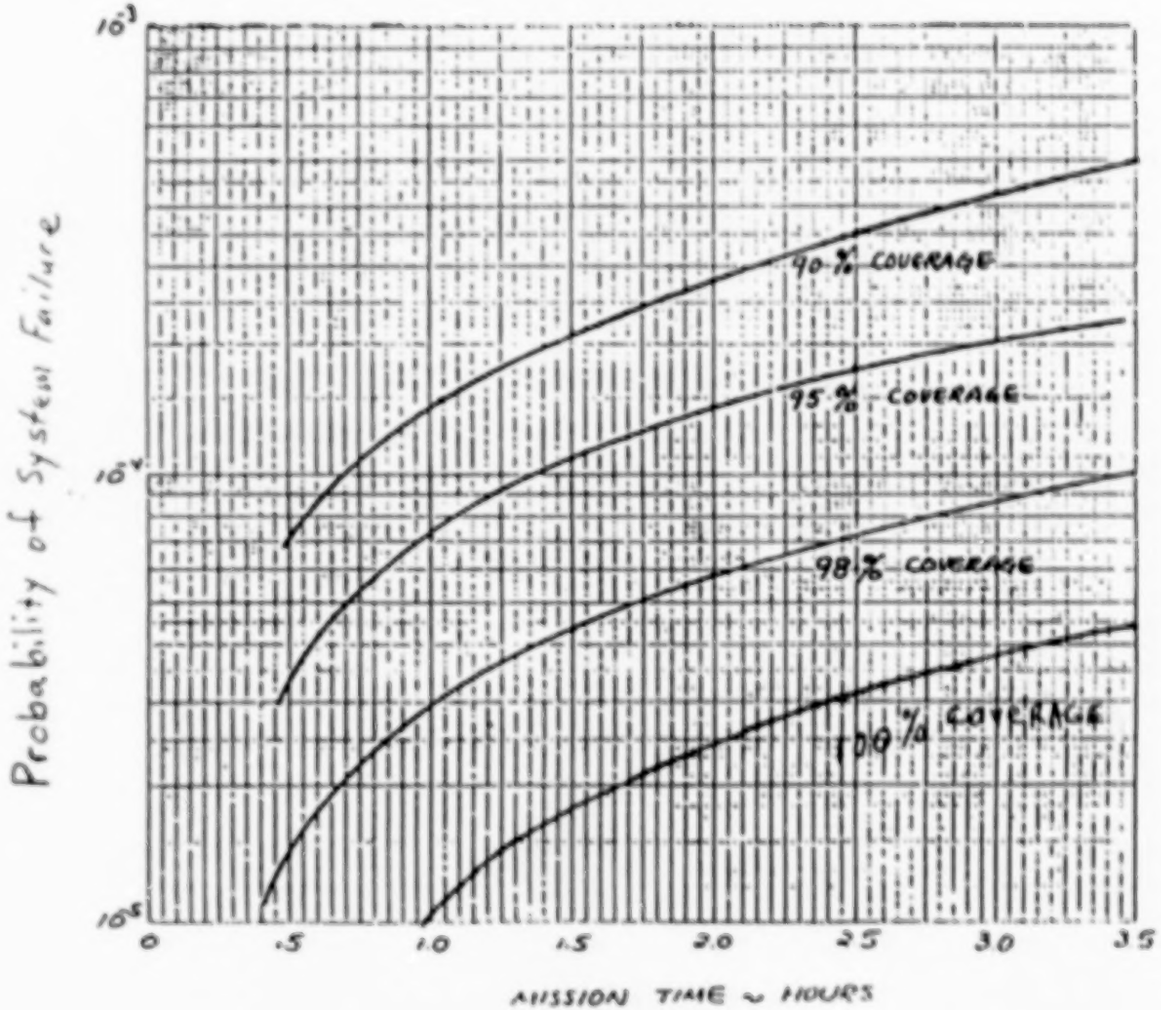


C : FAULT COVERAGE

GENERAL STRUCTURE OF CARE III AGGREGATE MODEL



SENSITIVITY OF FAULT COVERAGE



ORIGINAL PAGE IS
OF POOR QUALITY

INPUTS & OUTPUTS OF CARE III

INPUTS:

- FAULT HANDLING MODELS
- COMPONENT REDUNDANCY
- COMPONENT FAILURE RATES
- FAULT TREE (COMPONENT DEPENDANCY)
- RUN TIME PARAMETERS

OUTPUTS:

- PORTION OF UNRELIABILITY-VERSUS-TIME CAUSED BY
  - FAULT HANDLING
  - EXHAUSTION OF MODULES

TYPICAL CARE III RUN

CARE III NAMELIST INPUT	COMMENTS
$FLTTYP	- FAULT-HANDLING INPUT IDENTIFIER.
NFTYPS = 1,	- NUMBER OF FAULT MODELS (1 TO 5).
MARKOV = 1$	- SPECIFIES WHICH FAULT-HANDLING MODEL TO USE: CONSTANT TRANSITION RATE HOMOGENIUS MARKOVIAN MODEL (1) OR GENERAL SEMI-MARKOV MODEL (2).
$STAGES	- STAGE IDENTIFIER
NSTAGES = 5,	- NUMBER OF STAGES IN THE SYSTEM (1 TO 70).
N=2, 2*1, 4, 1,	- NUMBER OF IDENTICAL MODULES IN STAGE.
M=3*1, 2, 1$	- MINIMUM NUMBER OF MODULES NEEDED FOR STAGE TO BE OPERATIONAL.
$FLTCAT	- FAULT OCCURRENCE INPUT IDENTIFIER.
NFCATS = 5*1,	- NUMBER OF FAULT TYPES (1 TO 5).
RLM(1,1) = 5E-4,	PARAMETER X OF THE WEIBULL FAULT OCCURRENCE RATE FOR THE FAULT TYPE I FOR STAGE X (RLM(I,X)). THE TIME SCALE IS ALWAYS IN HOURS.
RLM(1,2) = 10E-4,	
RLM(1,3) = 2E-5,	
RLM(1,4) = 0.5E-6,	
RLM(1,5) = 200E-8$	
$RNTIME	- RUN TIME INPUT IDENTIFIER.
FT = 10.0,	- OPERATING TIME.
NSTEPS = 50$	- NUMBER OF TIME STEPS (17 TO 64). THE MORE STEPS USED, THE GREATER THE ACCURACY AND COMPUTATION TIME.

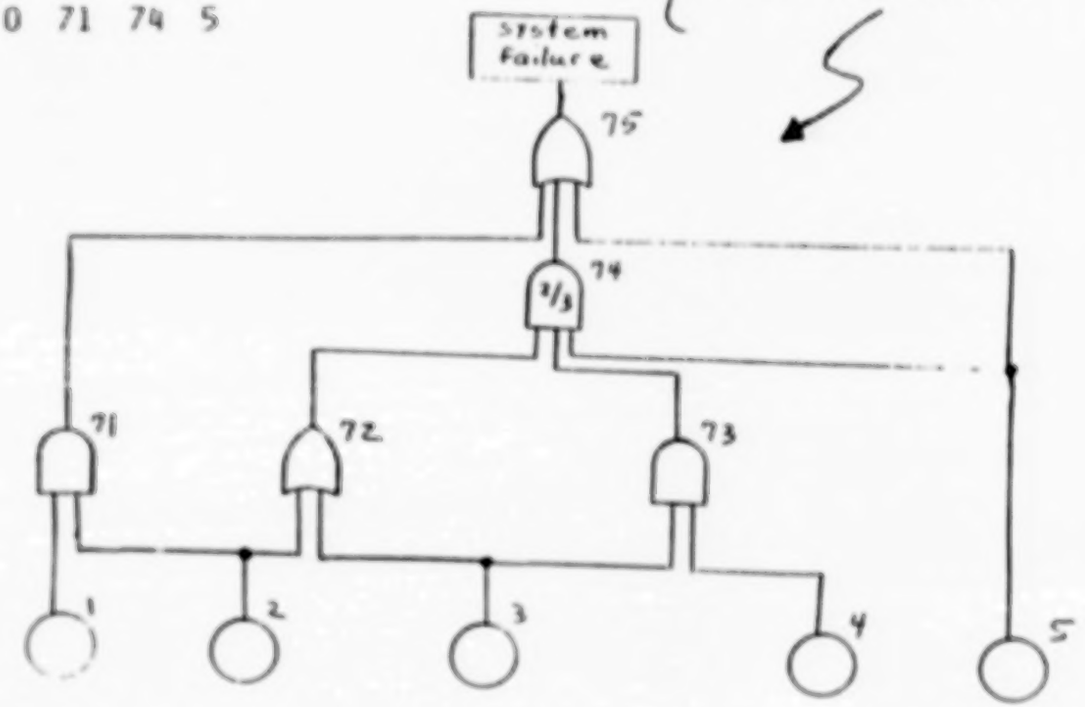
TYPICAL CARE III RUN (CONT.)

CARE III NAMELIST INPUT

```
SYSTEM FAULT TREE FOR SAMPLE
1  5  71  75
71  A  1  2
72  O  2  3
73  A  3  4
74  2  72  73  5
75  O  71  74  5
```

COMMENTS

- IDENTIFICATION LABLE.
- STAGE AND LOGIC RANGE IDENTIFICATION.
- LOGIC GATE IDENTIFICATION. UP TO 1930 GATES ALLOWED FOR MAXIMUM STAGES OF 70. (SEE SYSTEM FAULT TREE BELOW.)



CARE III SAMPLE RUN - INPUT

NAMELIST FORMAT *

LIST - DIRECTED FORMAT *

* - Only one format required

ORIGINAL PAGE IS
OF POOR QUALITY

CARE III SAMPLE RUN - SUMMARY

SUMMARY/ INFORMATION

Q SUM =

0.	2.67535225594E-12	1.67424783146E-11	5.24247876172E-11	7.40154438186E-11
1.09628422386E-10	1.31289827761E-10	1.66812125346E-10	1.86399278496E-10	2.24001758811E-10
2.47349372822E-10	2.89994918955E-10	3.15183134695E-10	3.57748786088E-10	3.87857182791E-10
4.25503644511E-10	4.58613830868E-10	4.93262613666E-10	5.16375648087E-10	5.61827279621E-10
5.86143852933E-10	6.28797112331E-10	6.53914891622E-10	6.96570355566E-10	7.21689361864E-10
7.64367282466E-10	7.89468817871E-10	8.32129878837E-10	8.57252881158E-10	8.99915855667E-10
9.25844446111E-10	9.67703826933E-10	9.92830890133E-10	1.03549442888E-09	1.06862194688E-09
1.10320781456E-09	1.12841613896E-09	1.17108269898E-09	1.19621222048E-09	1.23887940677E-09
1.26488955560E-09	1.30667725816E-09	1.33188784552E-09	1.37447602.24E-09	1.39968711885E-09
1.44227570288E-09	1.46748715866E-09	1.51007600816E-09	1.53528796772E-09	1.57787789436-09
1.60308910826-09				

P* SUM =

0.	2.34599567036-10	9.38396533946-10	2.11130836226-09	3.75357226966-09
5.86494583796-09	8.44558639956-09	1.14952513606-08	1.50141781896-08	1.90822840516-08
2.34599581516-08	2.83862176776-08	3.37819777336-08	3.96470000916-08	4.59809177866-08
5.27842684246-08	6.00564843286-08	6.77982056756-08	7.60007843116-08	8.46887949746-08
9.38376566986-08	1.03456803456-07	1.13543821286-07	1.24099996356-07	1.35126822556-07
1.46621670866-07	1.58585936556-07	1.71019126926-07	1.83921458156-07	1.97292927756-07
2.11133632986-07	2.25443271366-07	2.40222148156-07	2.55470136596-07	2.71187258866-07
2.87373503576-07	3.04029297196-07	3.21155625026-07	3.38750310126-07	3.56814720696-07
3.75346726736-07	3.94347988986-07	4.13817103246-07	4.33754691356-07	4.54160987366-07
4.75036814846-07	4.96389117866-07	5.18206330436-07	5.40489711366-07	5.63246041176-07
5.86470829346-07				

Q*P* SUM =

0.	2.37274919296-10	9.55139812266-10	2.16301300906-09	3.82758771346-09
5.97456626026-09	8.57671542716-09	1.16620634056-08	1.52025773886-08	1.92262858186-08
2.37869475236-08	2.86762125966-08	3.40970004716-08	4.00047488776-08	4.63637751696-08
5.32897728496-08	6.05870981516-08	6.82916602896-08	7.65227879956-08	8.52498182546-08
9.44236999516-08	1.04004888566-07	1.14196936896-07	1.24796866716-07	1.35804771916-07
1.47206626076-07	1.59375405366-07	1.71851256806-07	1.84778711036-07	1.98192842816-07
2.12058573436-07	2.26413977516-07	2.41214978246-07	2.56505631336-07	2.72247888796-07
2.88476791896-07	3.05157713336-07	3.22326787716-07	3.39946522326-07	3.58053600176-07
3.76609735286-07	3.95654666246-07	4.15140911096-07	4.35132167796-07	4.55664511466-07
4.76486898546-07	4.97856524216-07	5.19716414526-07	5.42024919236-07	5.64823918266-07
5.88073838546-07				

NUMBER OF FAILED STAGES	UNRELIABILITY AT 10.0000 HRS	PERFECT COVERAGE UNRELIABILITY AT 10.0000 HRS
P	1.60308910826-09	0.
1	*	5.86469891596-07
2	*	1.73776126626-12

TOTAL SYSTEM UNRELIABILITY AT 10.0000 HRS = 5.88073838546-07

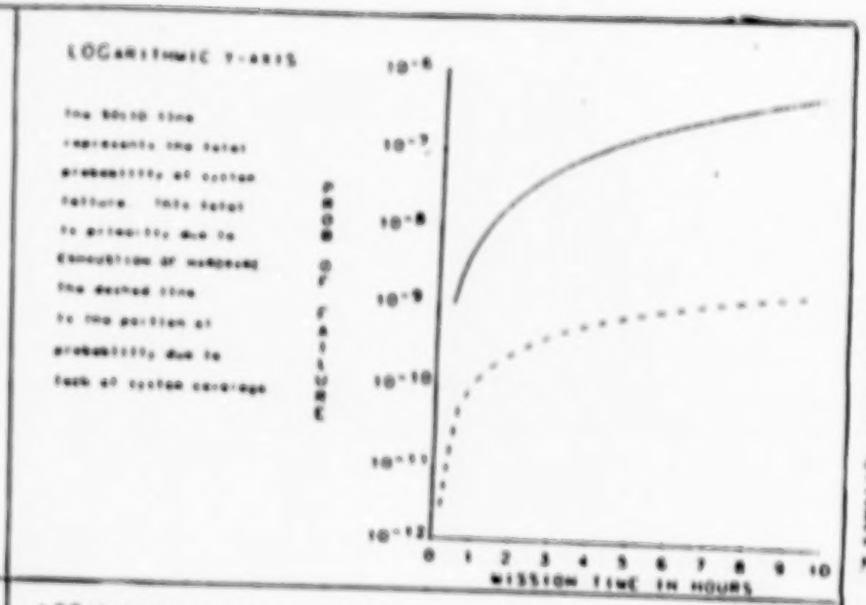
ORIGINAL PAGE IS OF POOR QUALITY

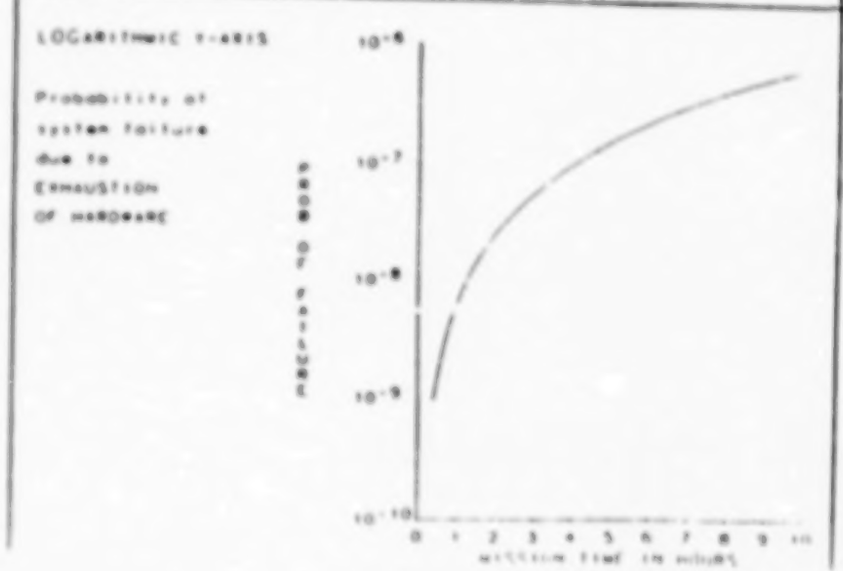
CARE III SAMPLE PLOTS

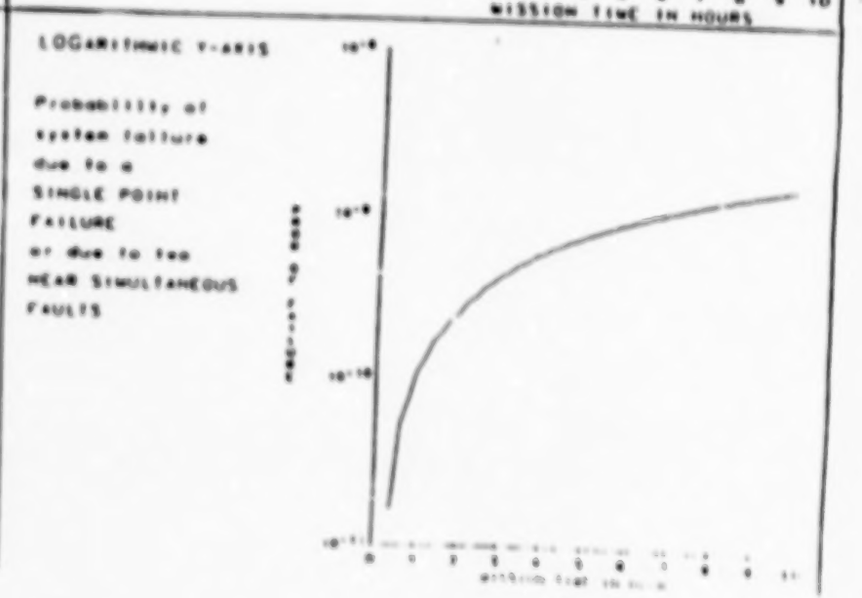
SUMMARY INFORMATION

Mission time = 10.0 hours

The probability of system failure due to a single point failure or due to two near simultaneous faults is - - -	.160E-8
The probability of system failure due to exhaustion of hardware is - - - - - - - -	.586E-6
total probability of system failure equals - -	.588E-6

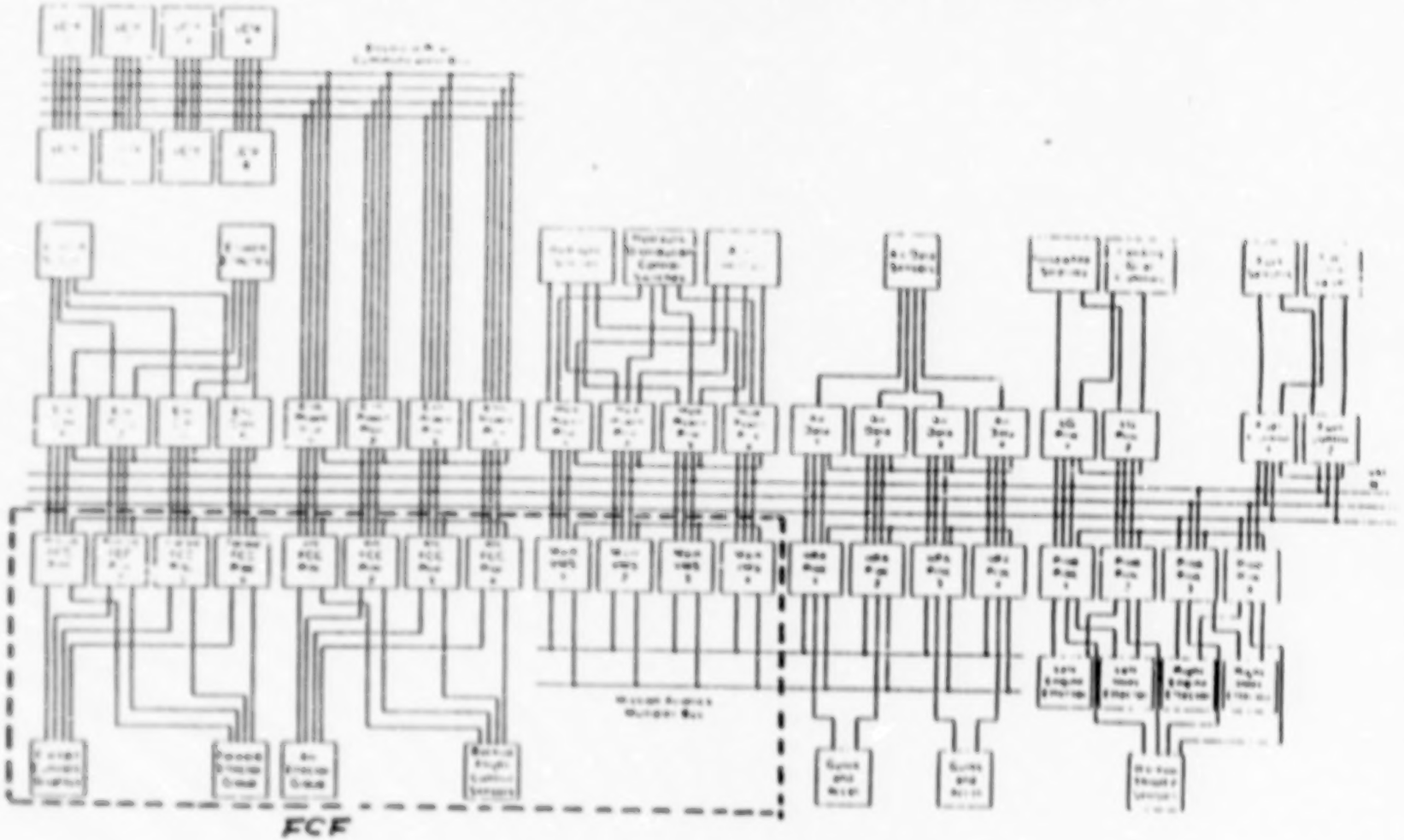

LOGARITHMIC Y-AXIS
the solid line represents the total probability of system failure. into total is probability due to exhaustion of hardware the dashed line is the portion of probability due to lack of system coverage
PROBABILITY OF FAILURE
10^{-6}
10^{-7}
10^{-8}
10^{-9}
10^{-10}
10^{-11}
10^{-12}
0 1 2 3 4 5 6 7 8 9 10
MISSION TIME IN HOURS




LOGARITHMIC Y-AXIS
Probability of system failure due to a SINGLE POINT FAILURE or due to two NEAR SIMULTANEOUS FAULTS
PROBABILITY OF FAILURE
10^{-6}
10^{-8}
10^{-10}

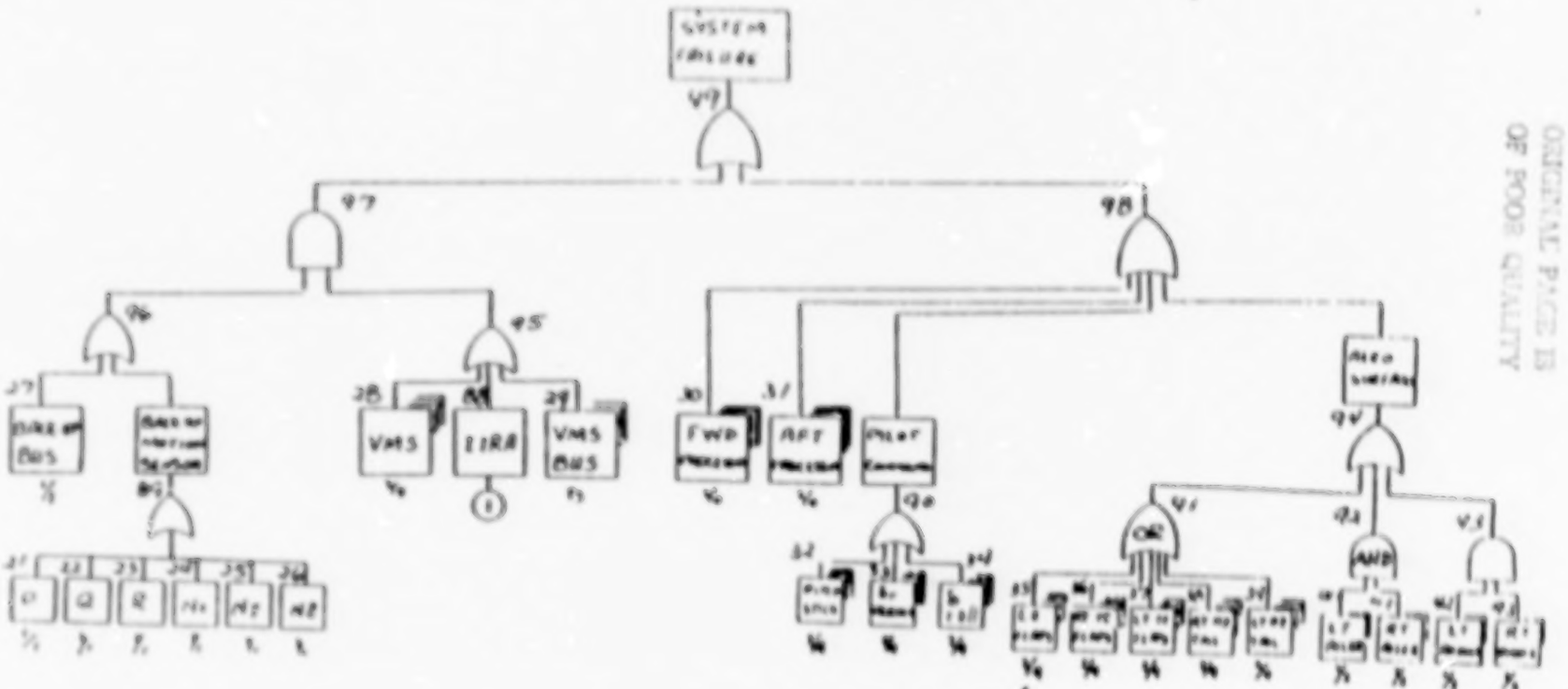
ORIGINAL PAGE IS
OF POOR QUALITY

VMS OVERVIEW - FLIGHT CONTROL FUNCTION (FCF) ANALYSIS



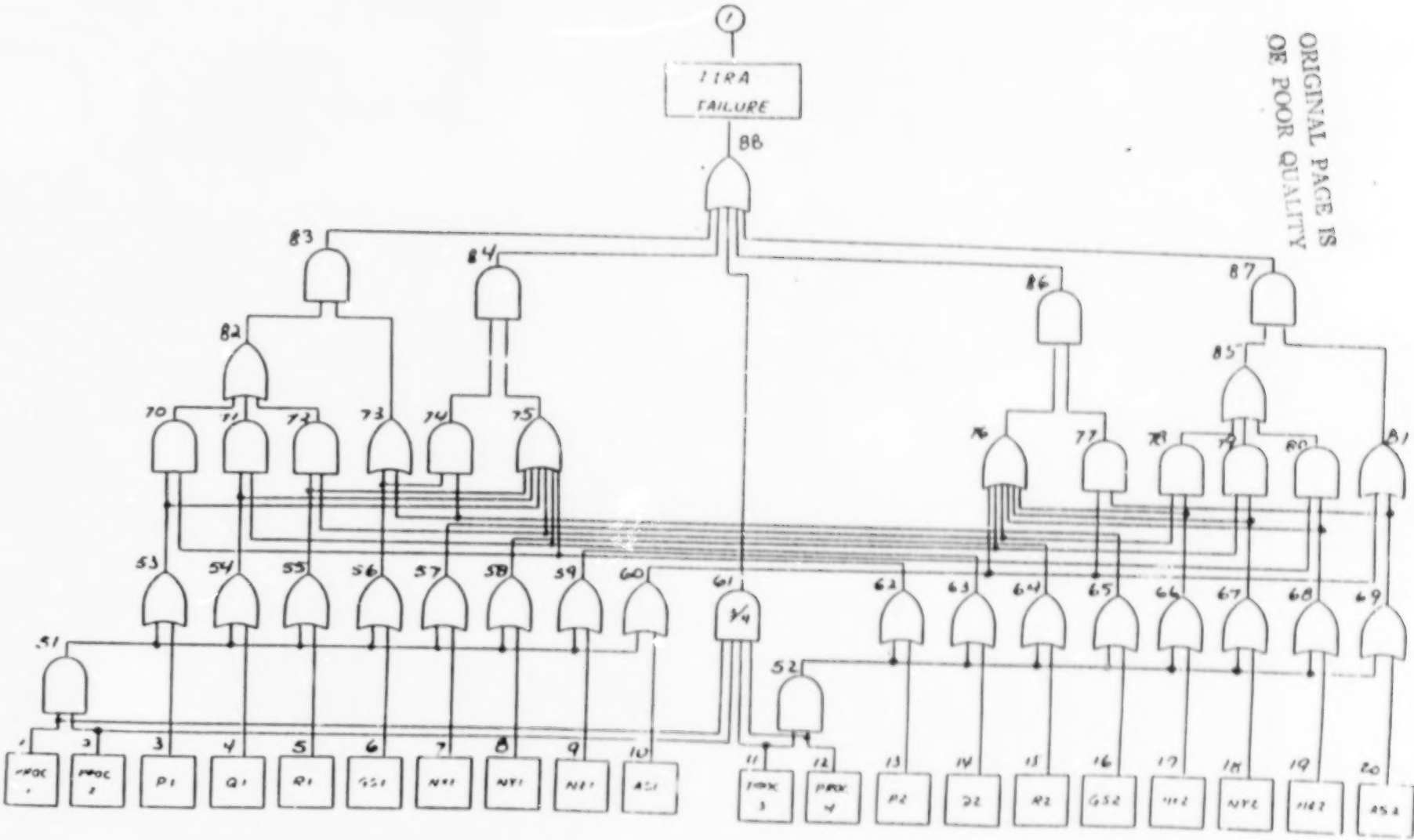
ORIGINAL PAGE IS
OF POOR QUALITY

FAULT TREE FOR FLIGHT CONTROL FUNCTION - MISSION ABORT



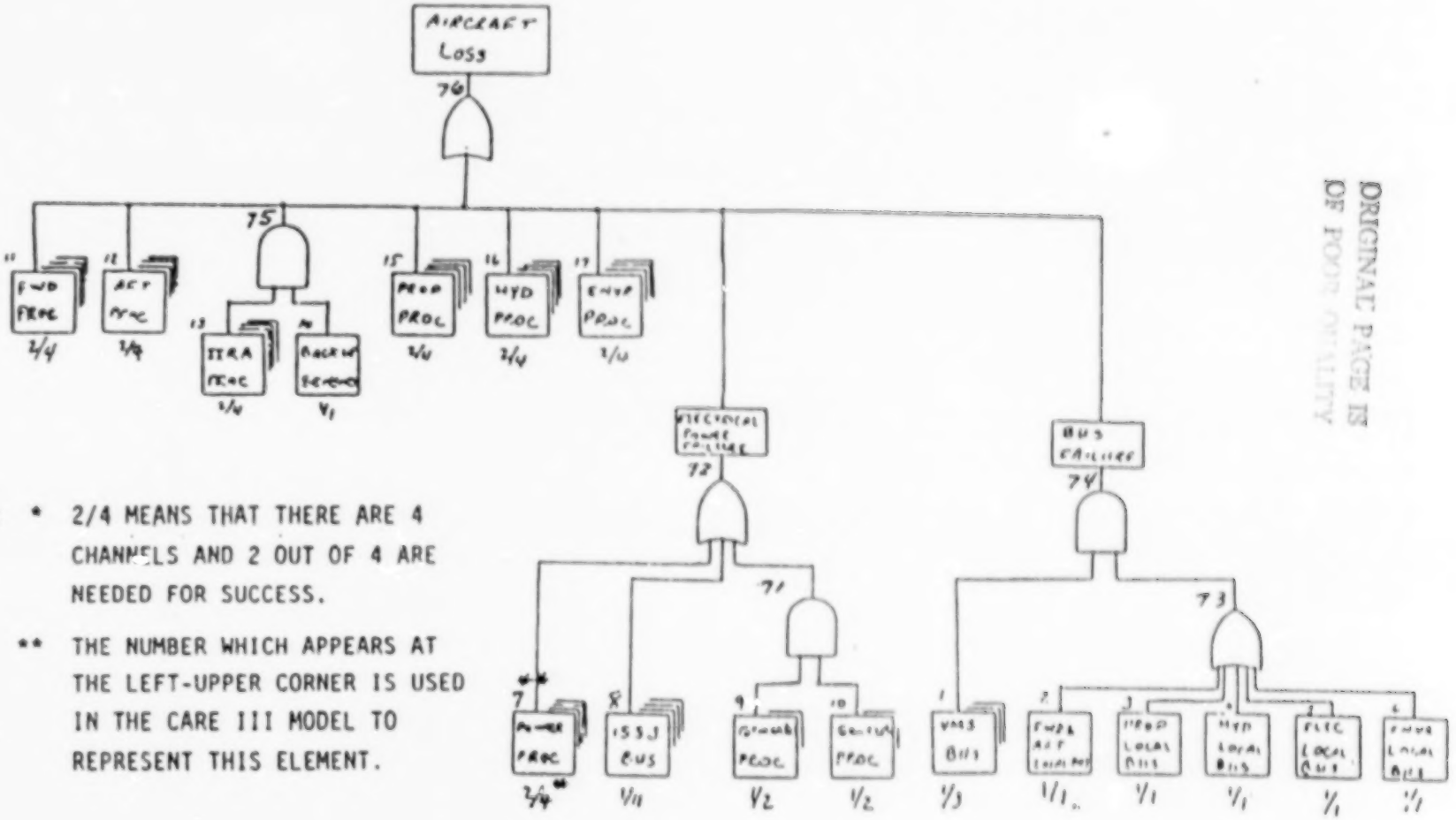
ORIGINAL PAGE IS OF POOR QUALITY

FAULT TREE FOR IIRA - MISSION ABORT



ORIGINAL PAGE IS
OF POOR QUALITY

FAULT TREE FOR VMS - AIRCRAFT LOSS



NOTE: * 2/4 MEANS THAT THERE ARE 4 CHANNELS AND 2 OUT OF 4 ARE NEEDED FOR SUCCESS.

** THE NUMBER WHICH APPEARS AT THE LEFT-UPPER CORNER IS USED IN THE CARE III MODEL TO REPRESENT THIS ELEMENT.

ORIGINAL PAGE IS
OF POOR QUALITY

ORIGINAL PAGE IS
OF POOR QUALITY

PROBLEMS OF CARE III

- FAULT HANDLING MODEL
  - IT DOES NOT DIFFERENTIATE SAFE SHUTDOWN FROM COMPLETE FAILURE
  - FAULT HANDLING MODEL DOES NOT VARY WITH REDUNDANCY LEVEL
- NO. OF COMPONENTS IS LIMITED TO 70
- COMPUTATION EFFICIENCY BECOMES INTOLERABLE FOR LARGE SYSTEM

OTHER TOOLS

- HARP (HYBRID AUTOMATED RELIABILITY PREDICTOR
  - AN ADVANCED VERSION OF CARE III
  - UNDER DEVELOPMENT AT DUKE UNIVERSITY FOR NASA LANGLEY RESEARCH CENTER

- GRAMP (GENERALIZED RELIABILITY AND MAINTAINABILITY PROGRAM)
  - DEVELOPED BY SYSTEMS CONTROL TECHNOLOGY (SCT)

- ARIES 82 (AUTOMATED RELIABILITY INTERACTIVE ESTIMATION SYSTEM, 1982 VERSION)

  DEVELOPED BY UCLA

ORIGINAL PAGE IS
OF POOR QUALITY

REFERENCES

1. BAVUSO, S.J., AND PETERSON, P. L., "CARE III MODEL OVERVIEW AND USER'S GUIDE, "NASA COSMIC #LAR-13349, APRIL 1985"

2. BAVUSO, S. J., "A USER'S VIEW OF CARE III", 1984 PROCEEDINGS ANNUAL RELIABILITY AND MAINTAINBILITY SYMPOSIUM, PP. 382-389

3. BRIDGMAN, M.S., AND NESS, W.G., "AUTOMATED ULTRARELIABILITY MODELS: A REVIEW," PP. 396-402

4. NAD MEMO #3832-86-202, "RELIABILITY MODELLING AND PREDICTION FOR THE VEHICLE MANAGEMENT SYSTEM (VMS)"

5. NAD MEMO #3832-86-187, "RELIABILTY MODELLING AND PREDICTION FOR THE FLIGHT CONTROL SYSTEM (FCS)"

ORIGINAL PAGE IS OF POOR QUALITY

EXAMPLES OF NONCONSERVATIVE RELIABILITY ESTIMATES GIVEN BY CARE III

October 7, 1987

Kelly J. Dotson

NASA Langley Research Center

BACKGROUND

- Primary task: test the SURE (Semi-Markov Unreliability Range Evaluator) program
- Comparison of SURE with CARE III for several different models and a range of parameter values
- For some problems, CARE III's unreliability estimates differed from the SURE bounds by several orders of magitude -- with no warnings or error messages
- This prompted a 4-way comparison among reliability analysis tools -- SURE, CARE III, PAWS, and STEM

OTHER RELIABILITY ANALYSIS TOOLS

SURE (Semi-Markov Unreliability Range Evaluator):

computes lower and upper bounds from algebraic formulas on the death-state probabilities of a semi-Markov model

PAWS (Pade Approximations With Scaling):

uses a combination of Pade approximations, scaling, and squaring techniques to compute a matrix exponential needed to solve the system of equations used to determine the death-state probabilities of a pure Markov model

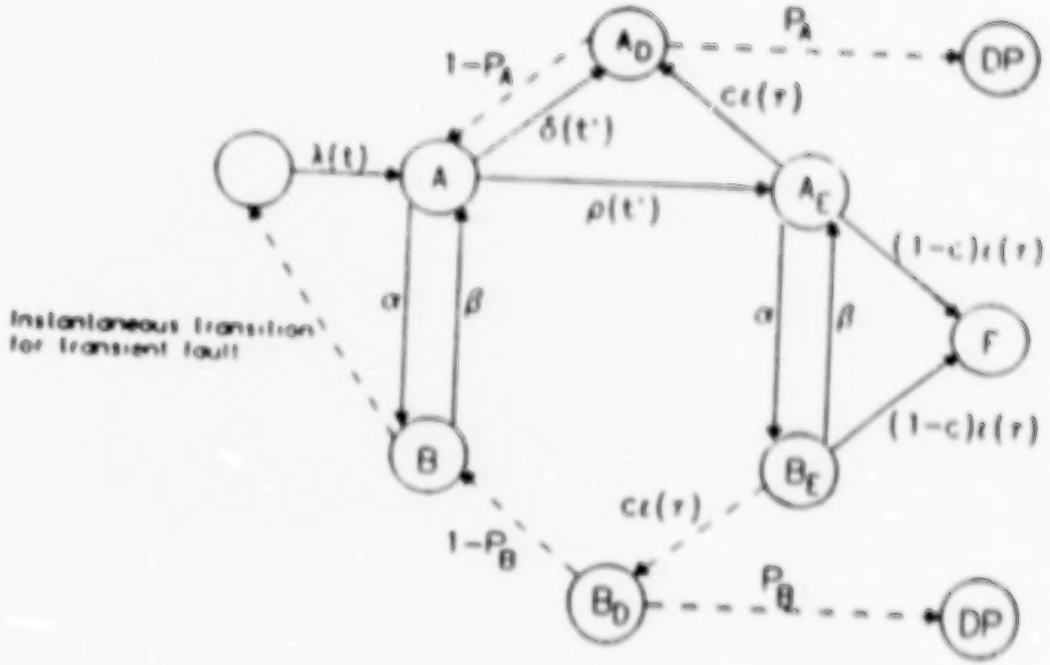
STEM (Scaled Taylor Exponential Matrix) :

uses Taylor series expansion techniques in calculating the matrix exponential needed to solve the system of equations used to determine the death-state probabilities of a pure Markov model

OBJECTIVES

- Point out some problems found in the CARE III program during the testing of the SURE program
- Demonstrate "fix" for some of these problems
- Stress need to compare results among reliability analysis tools

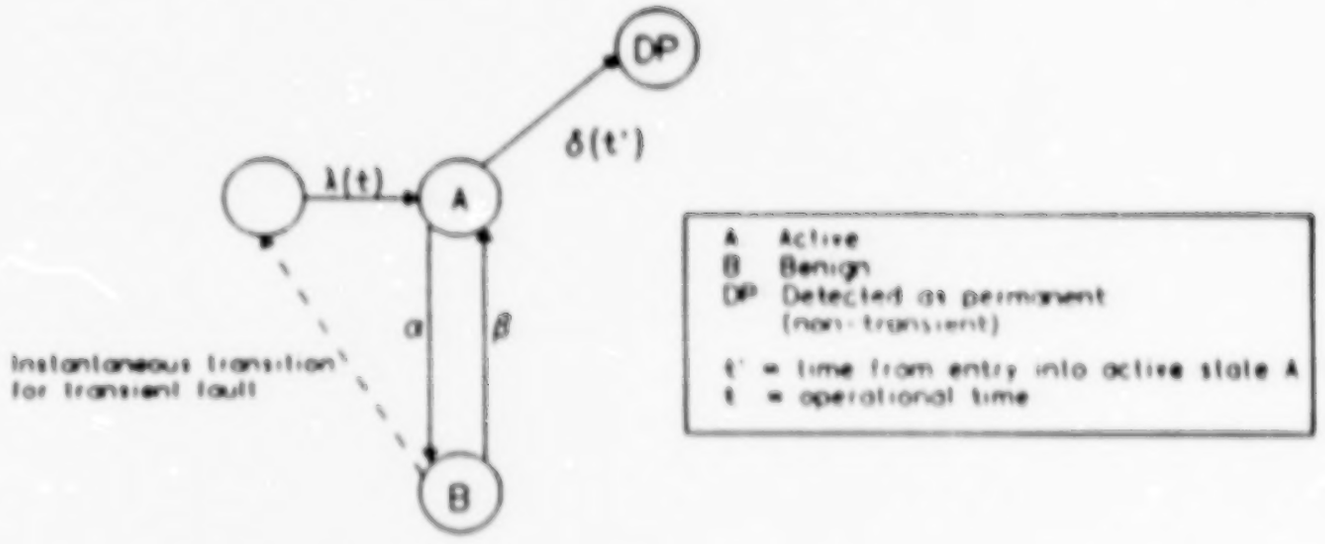
CARE III's Fault-handling Model



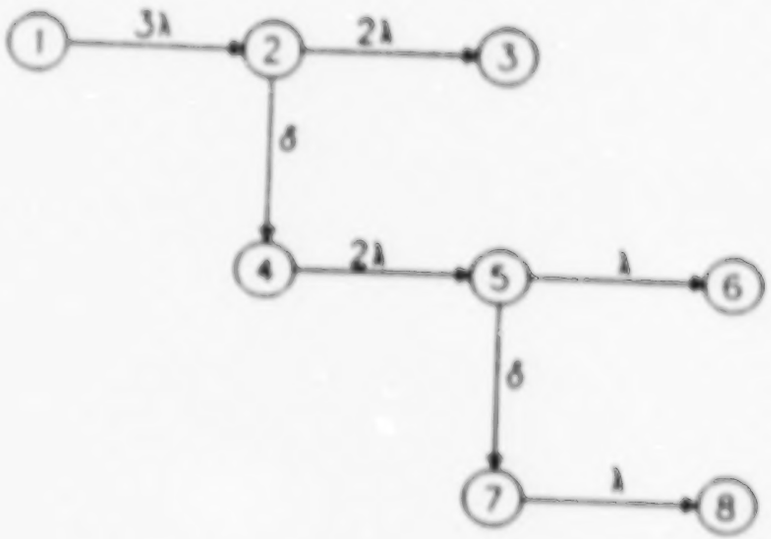
A Active
B Benign
D Detected
E Error
F Failure
DP Detected as permanent (non-transient)

t' = time from entry into active state A
t = operational time
τ = time from entry into error state E

CARE III's Fault-handling Model Simplified



Example 1: Triad with Permanent Faults



Comparison of SURE, PAWS, STEM, and CARE III for Example 1

PARAMETERS	SURE BOUNDS	Total System Unreliability Given by Each Tool PAWS	STEM	CARE III	CARE III*
λ= 1e-03 δ= 1e+02	(1.42254e-06, 1.60300e-06)	1.57267e-06 [9]	1.57267e-06 [4]	1.57588e-06	1.57588e-06
λ= 1e-04 δ= 1e+08	(9.98495e-10, 1.00001e-09)	9.98507e-10 [3]	9.98507e-10 [4]	9.98501e-10	9.98501e-10
λ= 1e-6 δ= 1e+2	(5.99422e-13, 6.01003e-13)	6.00388e-13 [9]	6.00388e-13 [4]	6.00658e-13	6.00658e-13
λ= 7e-7 δ= 1e+4	(3.25497e-15, 3.28301e-15)	3.28293e-15 [7]	3.28293e-15 [3]	3.29291e-15	3.29291e-15
λ= 6e-7 δ= 1e+4	(2.35560e-15, 2.37601e-15)	2.37595e-15 [7]	2.37595e-15 [3]	2.38329e-15	2.38329e-15
λ= 5e-7 δ= 1e+4	(1.61096e-15, 1.62500e-15)	1.62497e-15 [7]	1.62497e-15 [3]	1.24599e-168	1.63006e-15
λ= 1e-7 δ= 1e+2	(5.47623e-15, 6.00100e-15)	5.99499e-15 [9]	5.99499e-15 [4]	9.99999e-198	5.99766e-15
λ= 1e-7 δ= 1e+4	(6.04593e-17, 6.10000e-17)	6.09993e-17 [7]	6.09993e-17 [3]	9.99999e-198	6.12029e-17
λ= 1e-7 δ= 1e+8	(1.00599e-18, 1.00600e-18)	1.00600e-18 [3]	1.00600e-18 [4]	9.99999e-198	1.00602e-18
λ= 5e-7 δ= 1e+3	(1.47007e-14, 1.51250e-14)	1.51233e-14 [8]	1.51233e-14 [5]	1.24999e-168	1.51289e-14
λ= 1e-08 δ= 1e+02	(5.47543e-17, 6.00010e-17)	5.99410e-17 [9]	5.99410e-17 [4]	1.00000e-218	5.99676e-17

ORIGINAL PAGE IS
OF POOR QUALITY

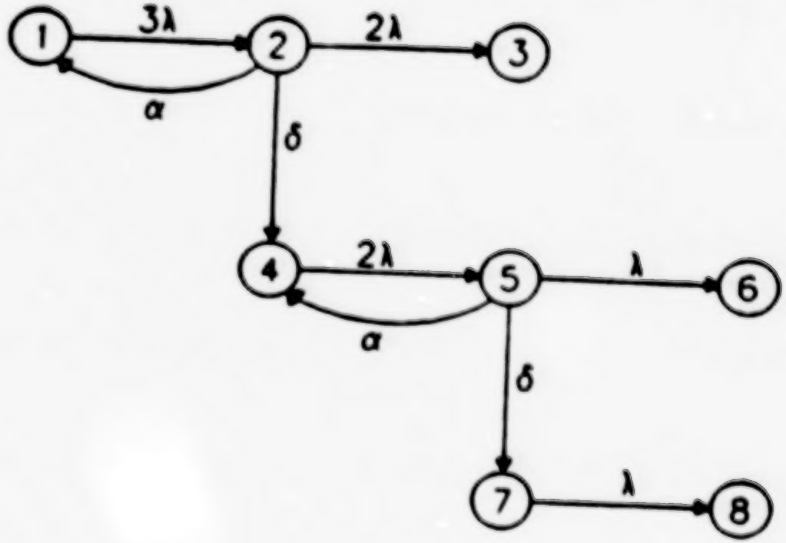
PSTRNC

- Run-time parameter used to limit the number of fault vectors that CARE III uses in computing the fault-handling unreliability. Only the fault vectors whose module depletion probability is less than PSTRNC will be included in the fault-handling unreliability calculation.

- The FT (flight time) parameter will affect how PSTRNC works

- "If too large of a value of PSTRNC is used, it is possible that some of the more significant $Q(t|\ell)$ values or possibly no $Q(t|\ell)$ values at all will be calculated. This value of PSTRNC in turn would make the value of QSUM on the output summary information page smaller than it should be."

Example 2: Triad with Transient Faults



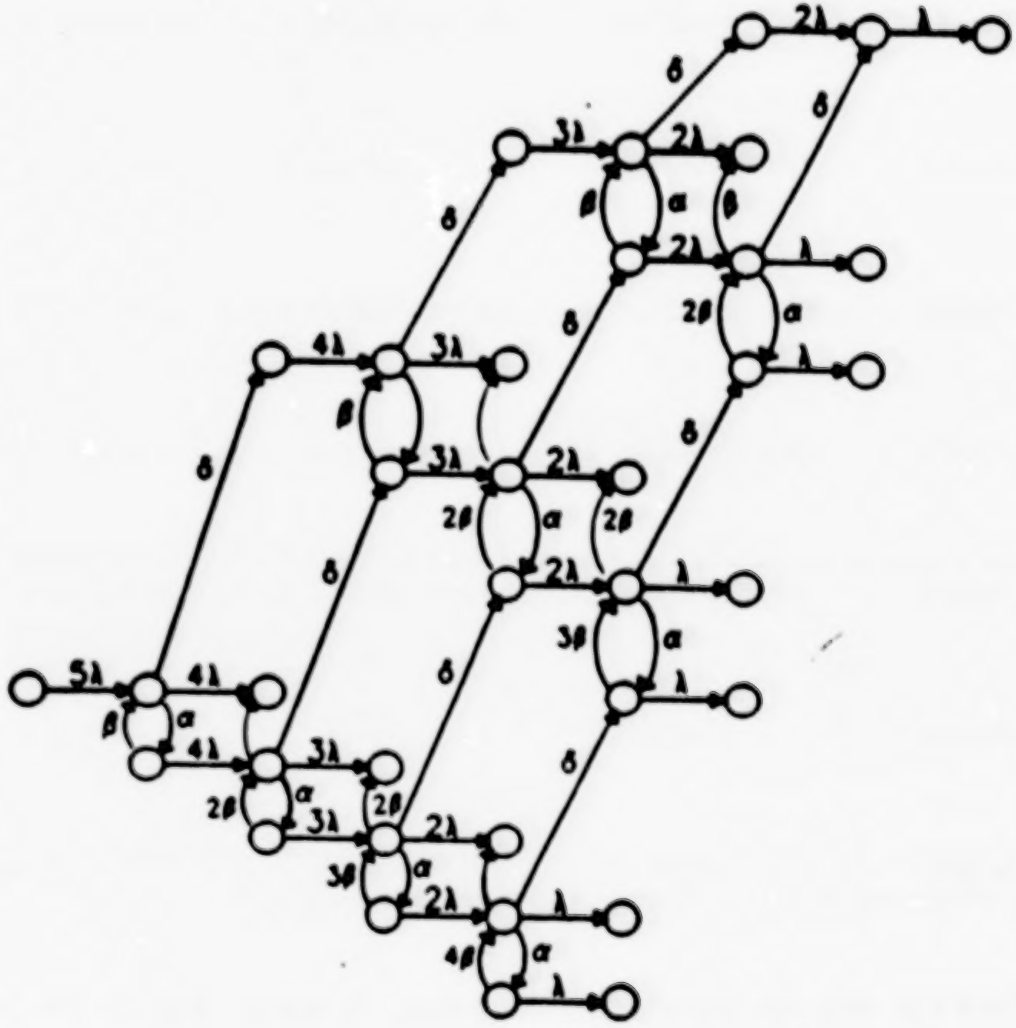
Comparison of SURE, PAWS, STEM, and CARE III for Example 2

PARAMETERS	Total System Unreliability Given by Each Tool: SURE BOUNDS	PAWS	STEM	CARE III
λ= 1e-03 δ= 1e+05 α= 1e+03	(9.65236e-07, 9.81015e-07)	9.66415e-07 [6]	9.66415e-07 [4]	9.63961e-07
λ= 1e-08 δ= 1e+07 α= 1e+02	(1.59975e-21, 1.59997e-21)	1.59997e-21 [4]	1.59997e-21 [3]	1.31233e-21
λ= 1e-04 δ= 1e+04 α= 1e-01	(1.05275e-09, 1.06001e-09)	1.05836e-09 [7]	1.05836e-09 [3]	1.03322e-09
λ= 1e-06 δ= 1e+03 α= 1e-02	(5.92900e-14, 6.09997e-14)	6.09922e-14 [7]	6.09922e-14 [5]	3.10625e-14
λ= 1e-04 δ= 1e+03 α= 1e+00	(1.55489e-09, 1.59771e-09)	1.59465e-09 [8]	1.59465e-09 [5]	1.29556e-09
λ= 1e-05 δ= 1e+02 α= 1e+05	(5.97717e-14, 5.99500e-14)	5.99410e-14 [6]	5.99410e-14 [4]	1.69753e-14

NOTE: The fault-handling model was designed for fast transients and intermittents, where α and β would be within 2 or 3 orders of magnitude of the other fault-handling parameters. Slower transients and intermittents are possible, but the user is cautioned to their use.

ORIGINAL PAGE IS
OF POOR QUALITY

Example 3: 5-Plex with Intermittent Faults



Comparison of SURE, PAWS, STEM, and CARE III for Example 3

PARAMETERS	SURE BOUNDS	Total System Unreliability Given by Each Tool PAWS	STEM	CARE III	CARE III*
λ= 1e-6 α= 3.6e-3 β= 1e-2 δ= 3.6e+6	(5.55288e-17, 5.55564e-17)	5.55550e-17 [4]	5.55550e-17 [2]	5.57649e-17	5.57658e-17
λ= 1e-6 α= 3.6e-2 β= 1e+1 δ= 3.6e+2	(5.29698e-13, 5.55674e-13)	5.55449e-13 [7]	5.55449e-13 [4]	5.57028e-13	5.57036e-13
λ= 1e-6 α= 3.6e-1 β= 1e-1 δ= 3.6e+2	(5.29530e-13, 5.55417e-13)	5.55249e-13 [7]	5.55249e-13 [4]	5.53959e-138	5.53967e-138
λ= 2e-7 α= 3.6e-3 β= 3.6e-2 δ= 3.6e+1	(1.90313e-13, 2.22230e-13)	2.21589e-13 [8]	2.21589e-13 [6]	3.19998e-298	2.21615e-13
λ= 1e-7 α= 3.6 β= 1e-1 δ= 3.6e+2	(5.28272e-15, 5.54082e-15)	5.53926e-15 [7]	5.53926e-15 [4]	9.99998e-318	5.50788e-158
λ= 1e-8 α= 1e-1 β= 1e+2 δ= 1e+6	(1.99821e-20, 2.00000e-20)	2.00000e-20 [4]	2.00000e-20 [3]	1.00000e-358	2.00275e-20
λ= 1e-4 α= 1e+2 β= 1e+1 δ= 1e+3	(2.13068e-09, 2.19804e-09)	2.19131e-09 [6]	2.19131e-09 [5]	2.18797e-098	2.18797e-098

ORIGINAL PAGE IS
OF POOR QUALITY

SUMMARY

- Examples were elementary constructions in modeling fault-tolerant computer systems
- Some of the CARE III estimates for unreliability were not only inaccurate but were also not conservative
- No warning or error messages were output by CARE III for any of the given test cases

CONCLUSIONS

- In cases where the fault-arrival rate is very very small, decreasing the runtime parameter PSTRNC seems to enable CARE III to produce a conservative reliability estimate in models with either permanent or intermittent faults

- In the transient error cases, there is no obvious cause of CARE III's inaccuracies nor is there currently any "fix" for the problem

- There are many subtleties involved in modeling a system with CARE III. One should not rely on CARE III to warn the user that CARE III's reliability estimate may not be conservative

- Whenever possible, compare estimates

HARP

October 7, 1987

Salvatore J. Bavuso

NASA Langley Research Center

HARP
RELIABILITY
AUTOMATED
PREDICTOR
HYBRID

HARP

- Fourth Generation Computer-Aided Reliability Engineering Tool

- Codeveloped by Duke University, LaRC, and Clemson University

OUTLINE

- Research Objective
- Combined Analytic Simulative Approach
- H A R P (Hybrid Automated Reliability Predictor)
- Status and Future Work

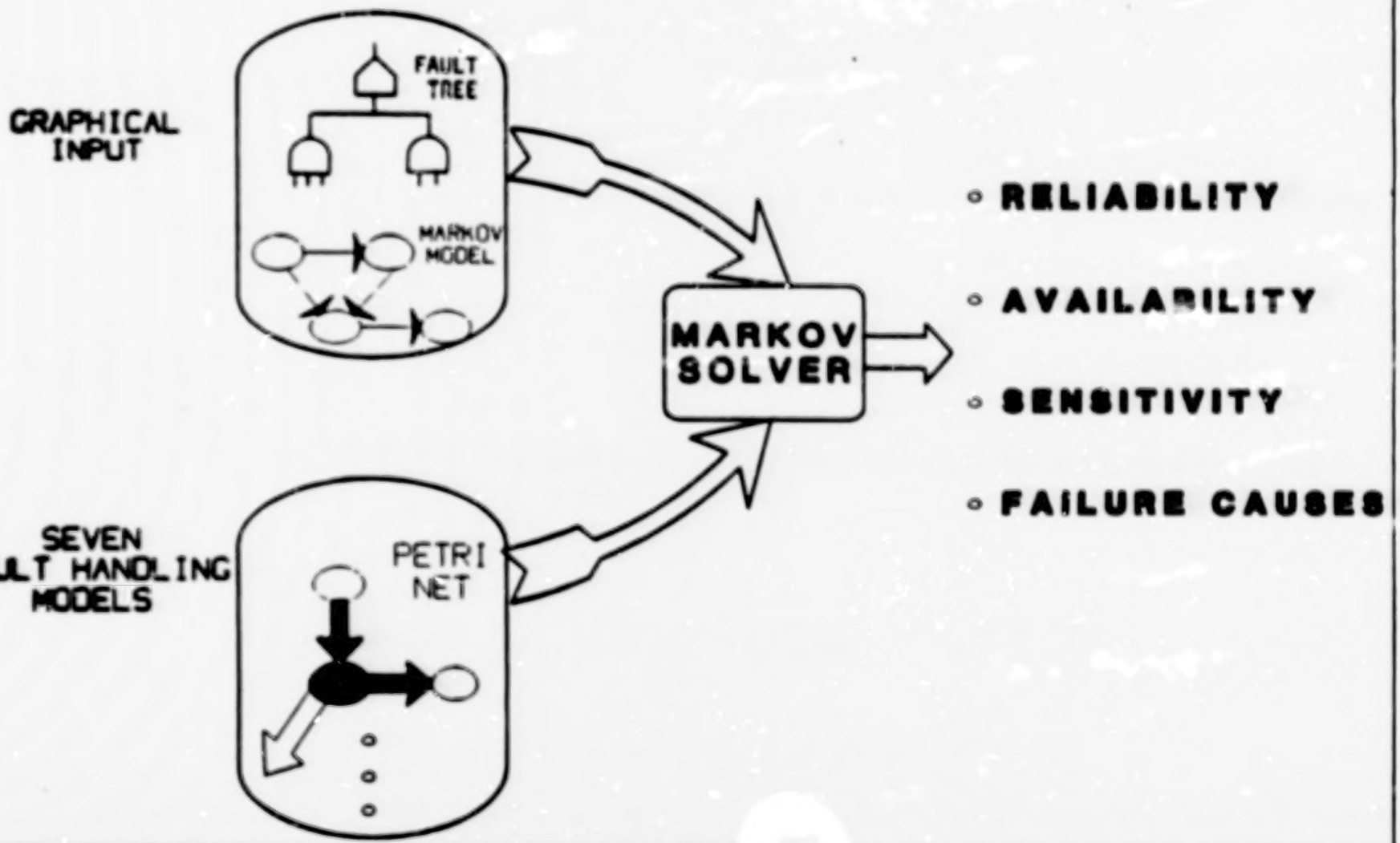
RESEARCH OBJECTIVE

Provide a Reliability Assessment Capability to:

- Estimate reliability of systems under repair (Availability)
- Automatically generate a complex Markov chain model from a less complex fault tree
- Furnish flexible Fault-Handling Models
- Compute sensitivity bounds for trade analyses

HYBRID AUTOMATED RELIABILITY PREDICTOR (HARP)

A FLEXIBLE RELIABILITY ESTIMATION TOOL

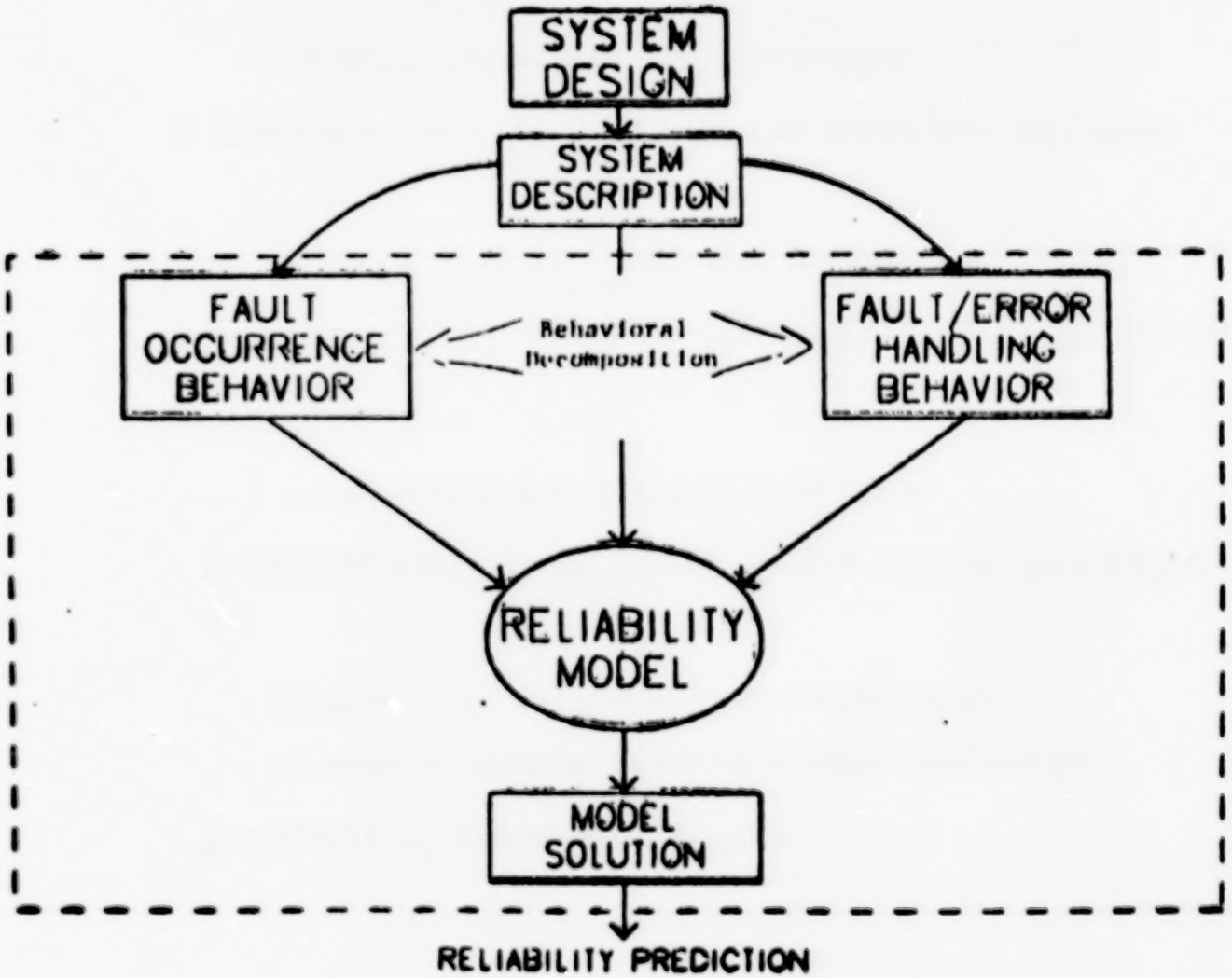


COMBINED ANALYTIC SIMULATIVE APPROACH

- **Behavioral Decomposition**
  - To reduce system analytic model complexity attributed to fault-handling complexity
- **Decomposition of Fault Occurrence Behavior**
  - To use piece-parts life testing data
- **Simulation of System Fault-Handling Behavior**
  - As input data to composite model
- **Aggregation of Subsystem Analytic Models**
  - To form composite analytic model
- **Analytic Solution**
  - To predict system reliability

HARP

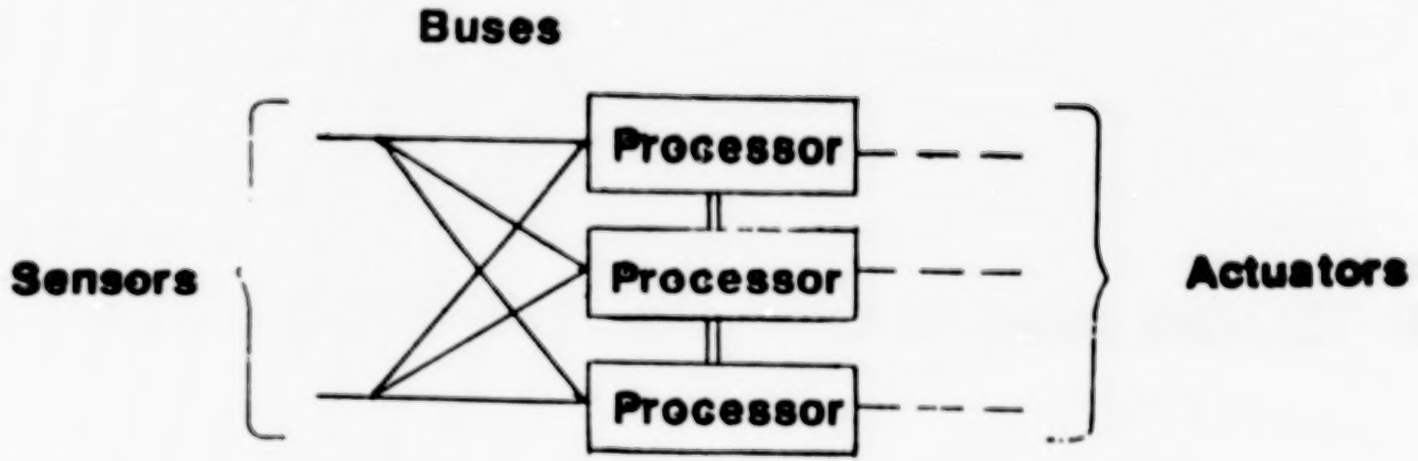
(HYBRID AUTOMATED RELIABILITY PREDICTOR)



EXAMPLE SYSTEM

Signal Flow Representaton

3-Processor/2-Bus System



FAULT OCCURRENCE AND REPAIR MODEL (FORM)

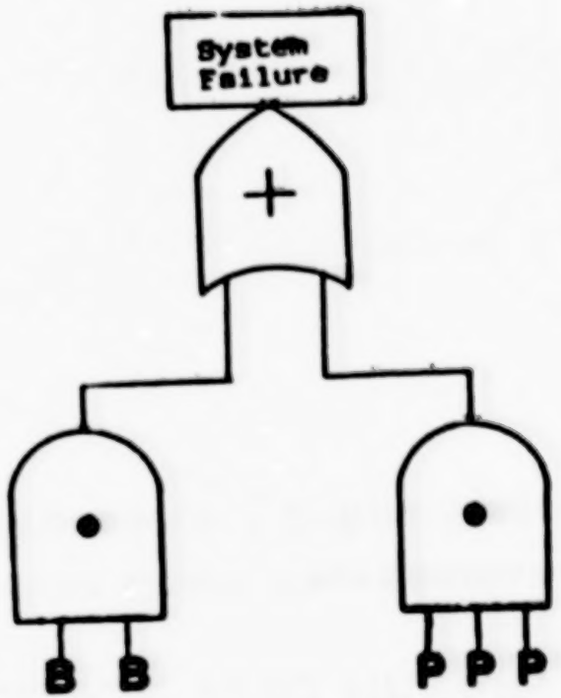
ORIGINAL PAGE IS
OF POOR QUALITY

- Fault Tree
- Markov Chain
- Hierarchical State Diagram

FAULT OCCURRENCE AND REPAIR MODEL (FORM)

Fault Tree Representation

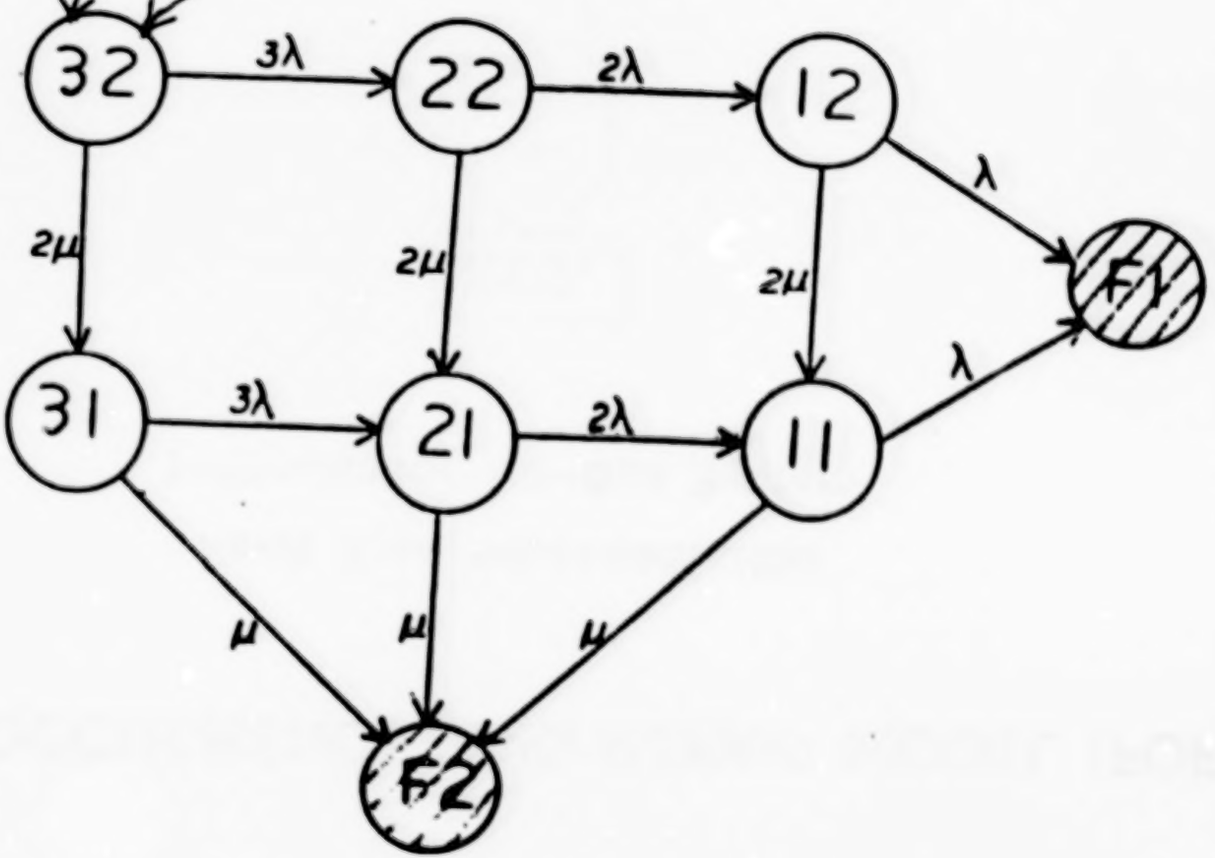
3-Processor / 2-Bus System



FAULT OCCURRENCE AND REPAIR MODEL (FORM)

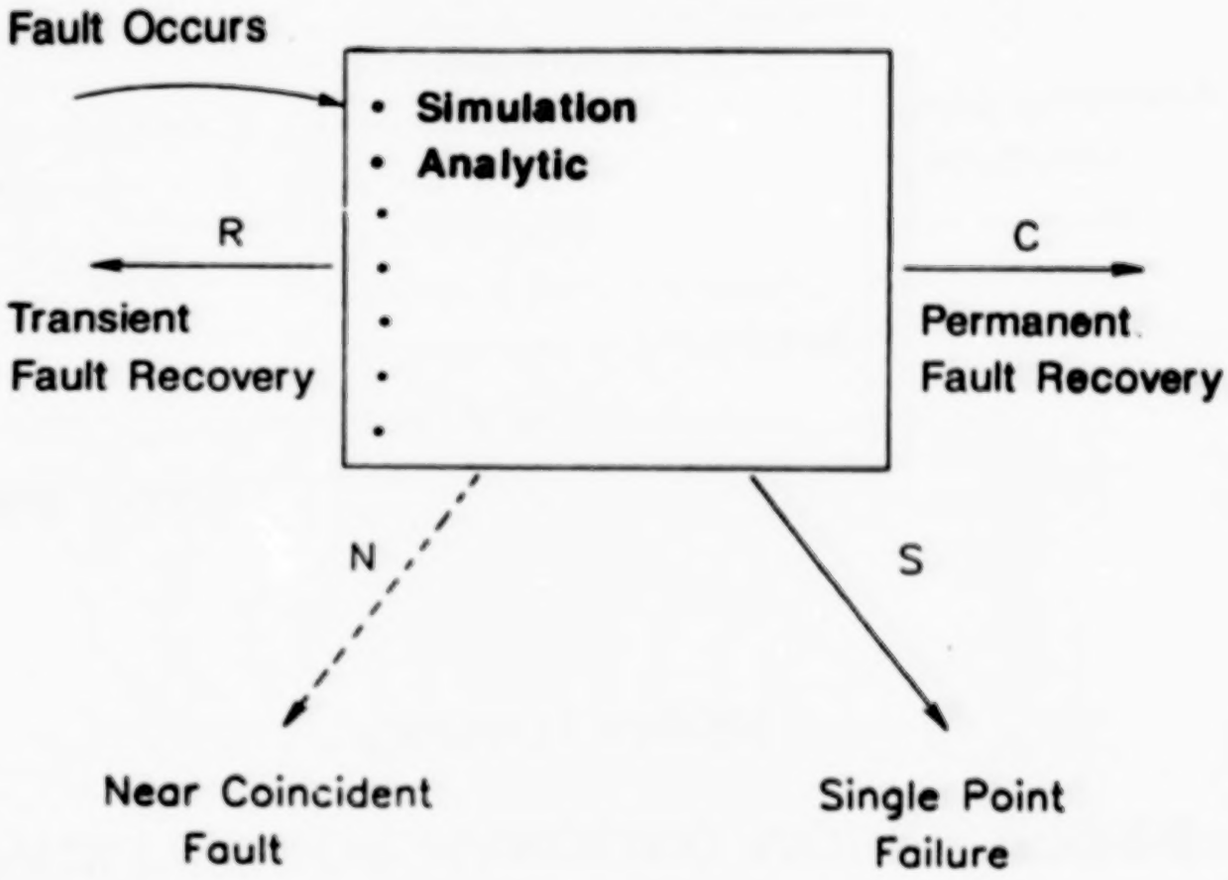
Markov Chain Representation

3-Processor / 2-Bus System



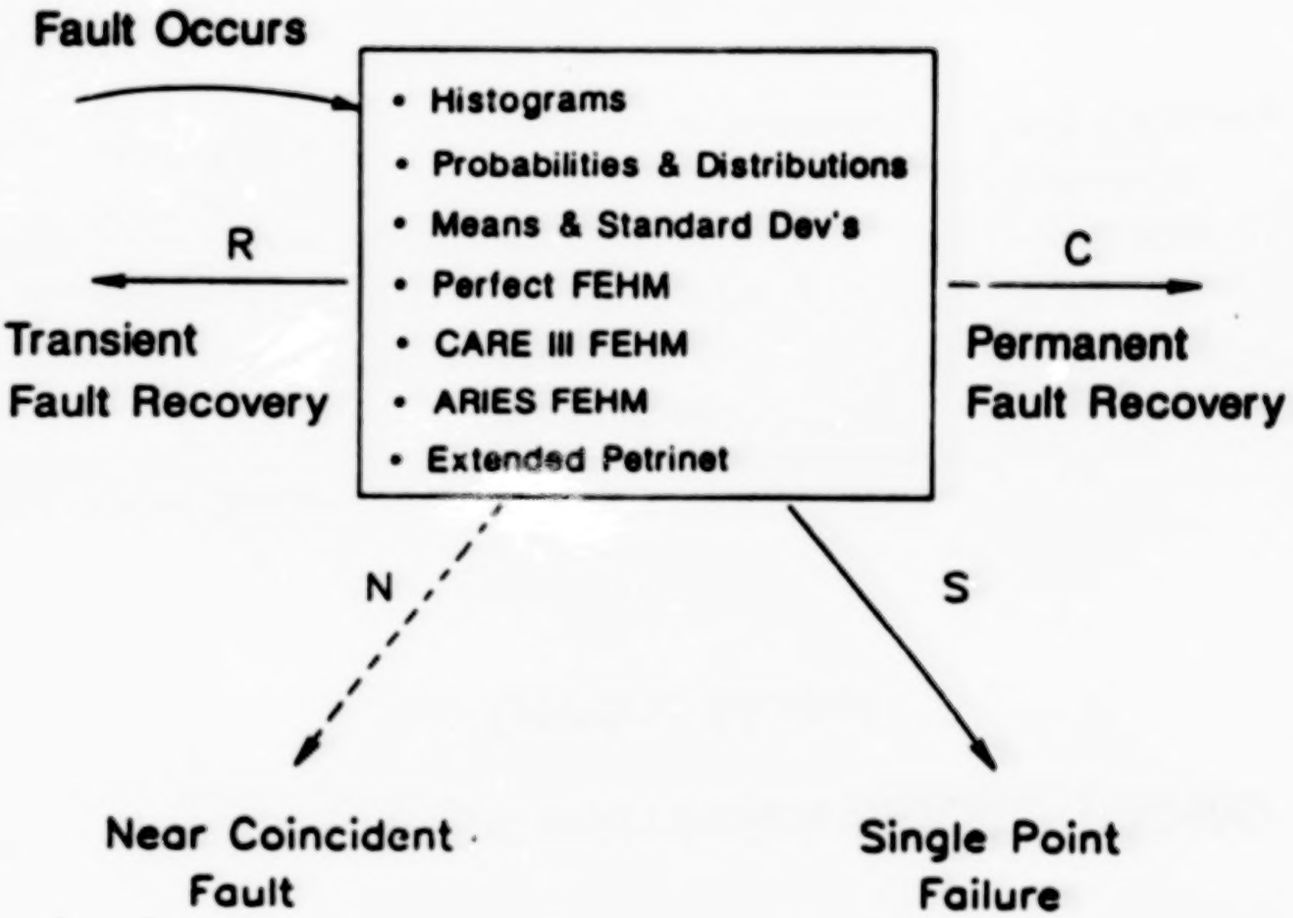
FAULT/ERROR HANDLING MODEL (FEHM)

Generic Model

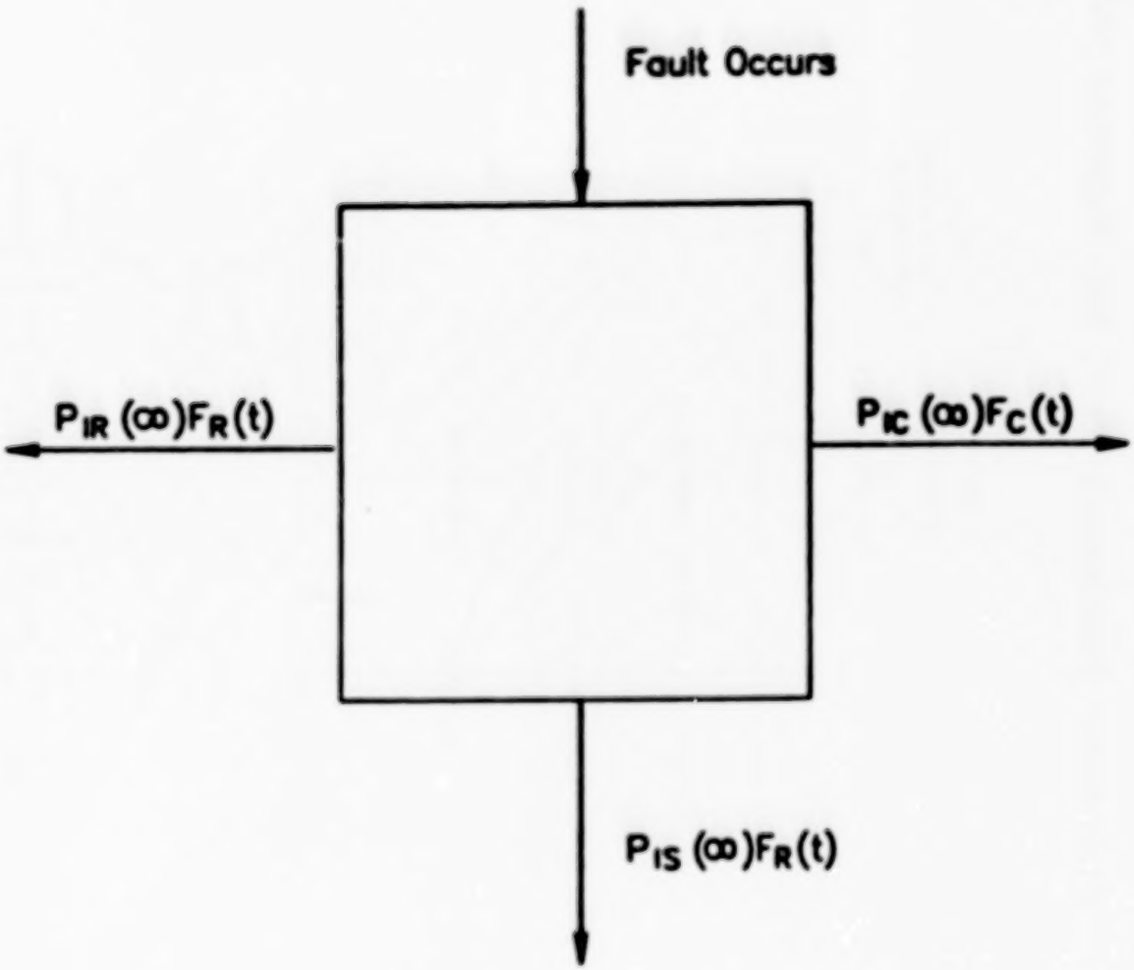


FAULT/ERROR HANDLING MODEL (FEHM)

Generic Model



Probabilities and Distributions



ORIGINAL PAGE IS
OF POOR QUALITY

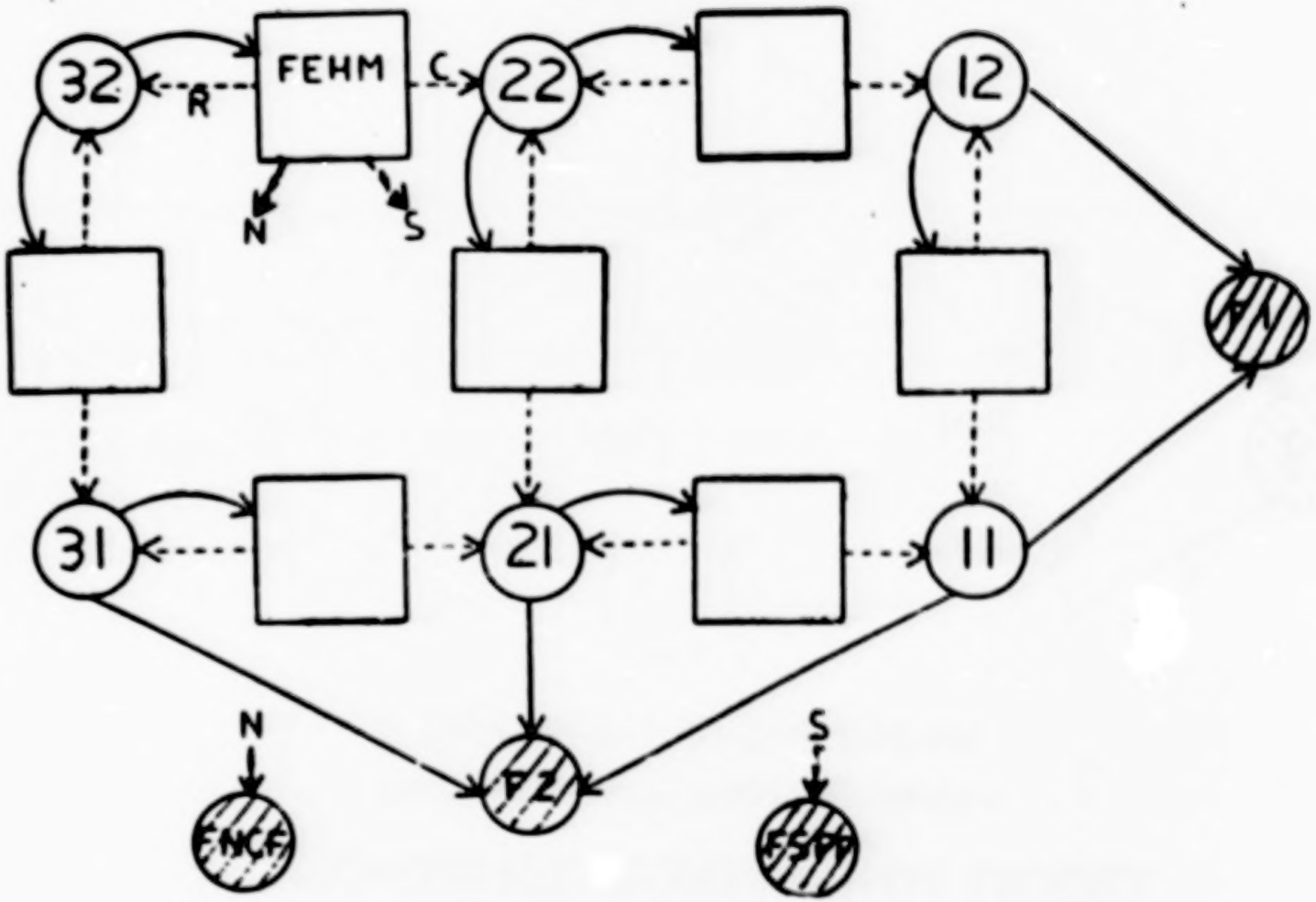
ORIGINAL PAGE IS
OF POOR QUALITY

FEHM: Fault/Error Handling Model

Extended Stochastic Petri Net Representation

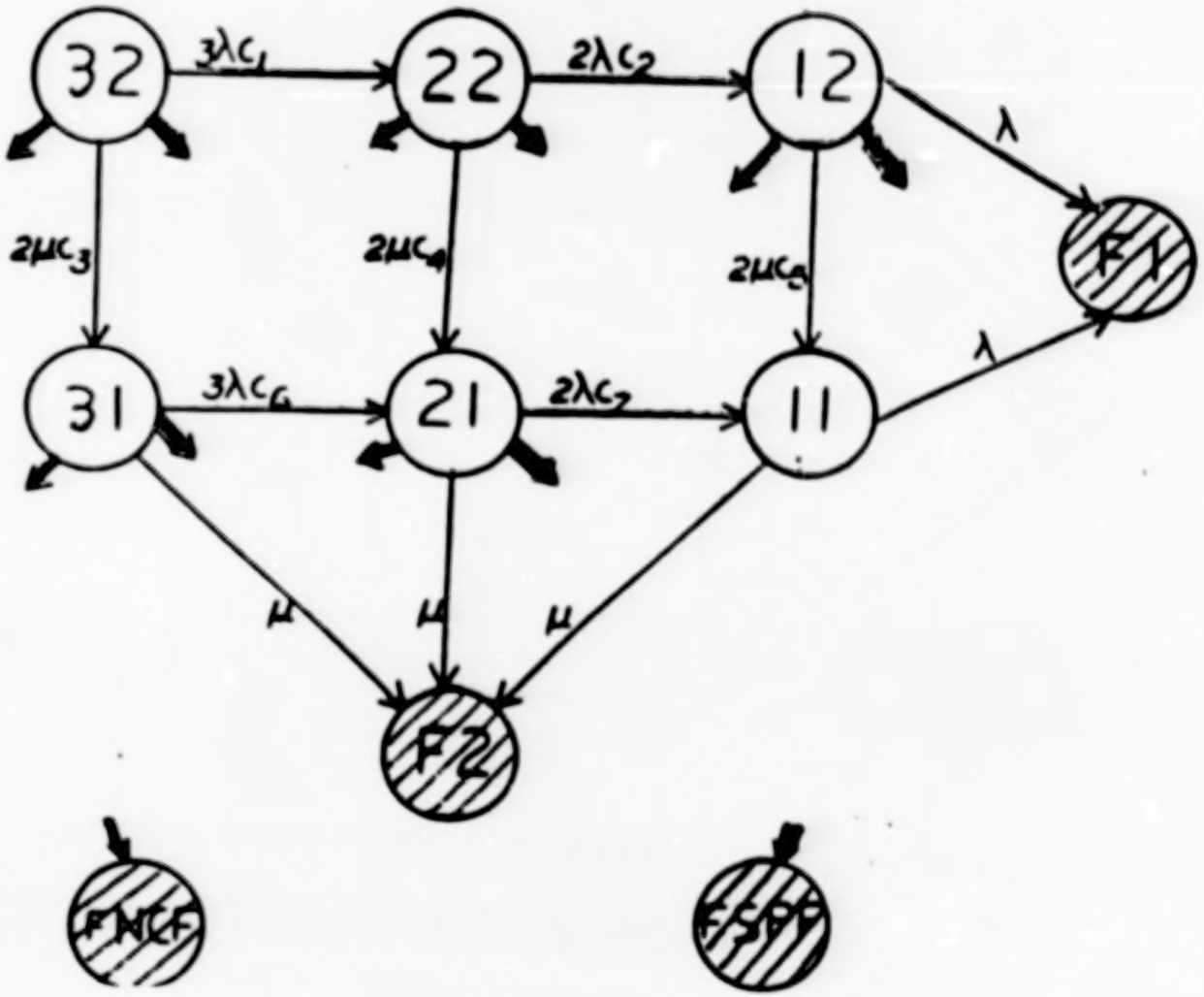
COMBINED FORM/FEHM MODEL

Markov Chain Representation

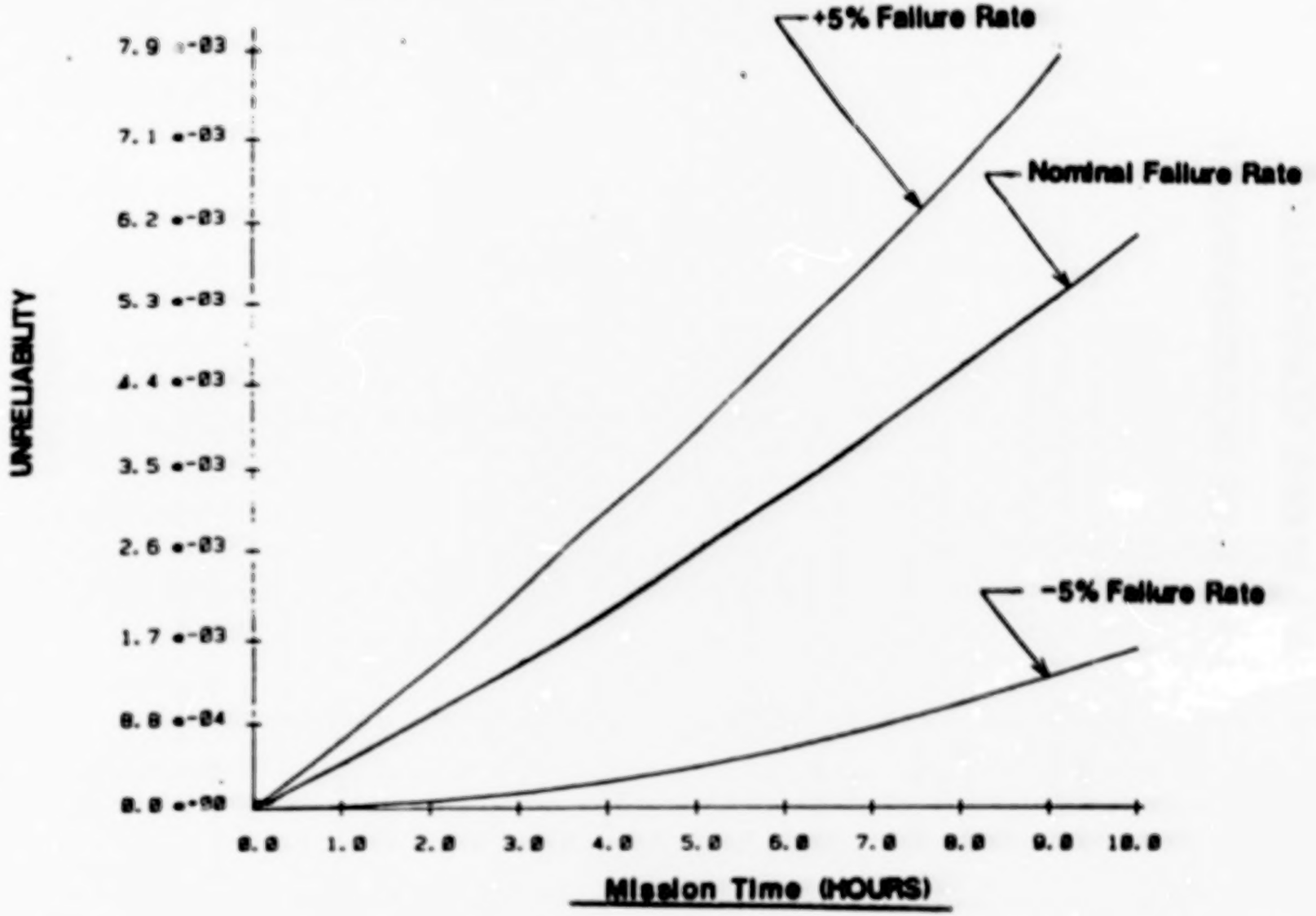


COMBINED FORM/FEHM MODEL

Markov Chain Representation
3 Processor / 2-Bus System

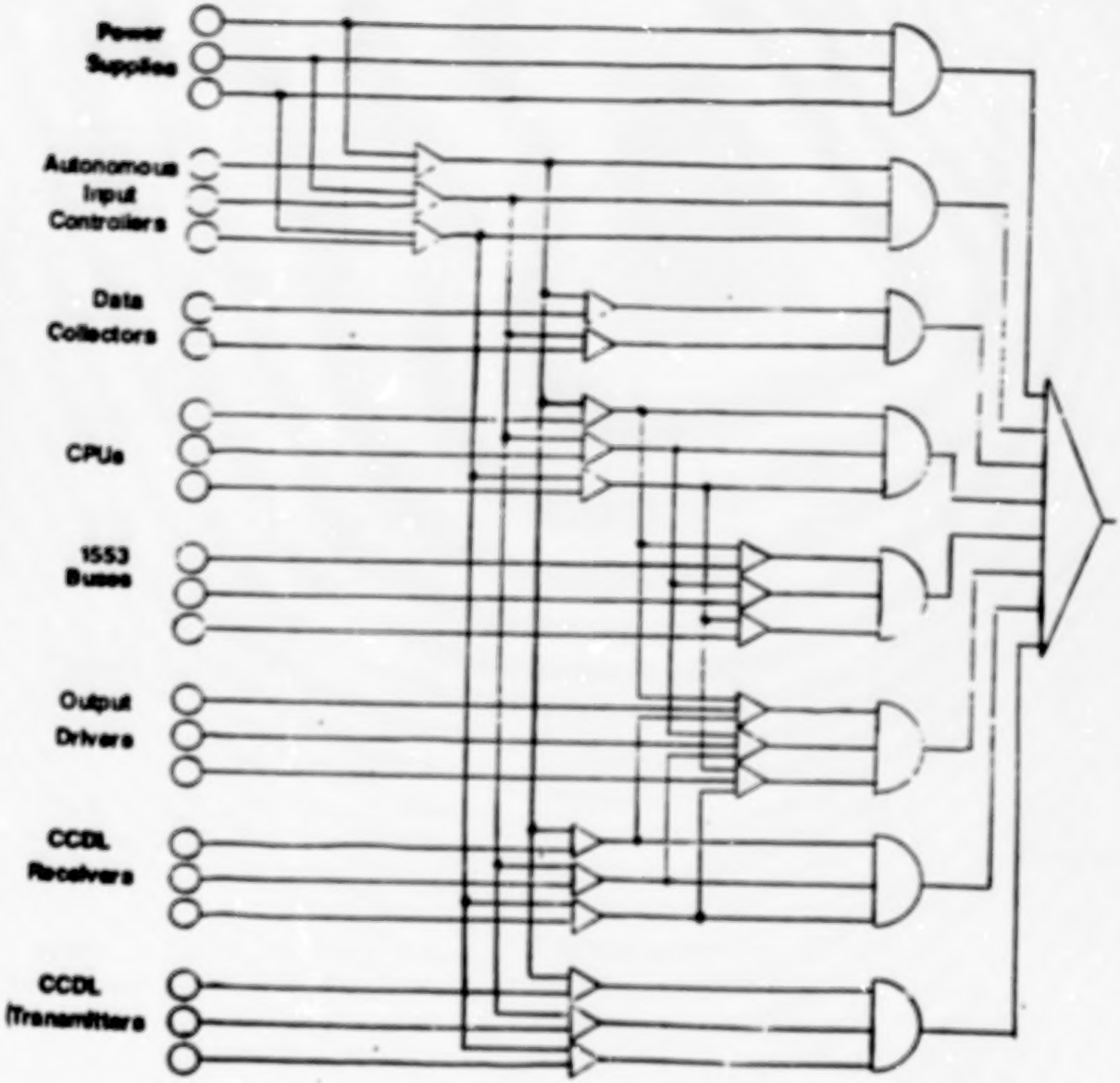


UNRELIABILITY OF 3-PROCESSOR / 2-BUS SYSTEM
(With Sensitivity Bounds)



JET ENGINE CONTROLLER

FAULT TREE REPRESENTATION



DE BOOK QUALITY

LIMITATIONS

- Some Classes of Computer Networks, i.e.,
  AIPS (Advanced Information Processor System)

- Software Reliability

- Markov Chain State Explosion Due to Fault Occurrence and Repair Model
  - 25,000 States and 500,000 Transitions
  - Need Equivalent to 500,000+ States

WEIBULL REFERENCES

Reliability Prediction for Spacecraft by Herbert Hecht and Myron Hecht. RADC-Technical Report 85-229. December 1985 Rome Air Development Center, Air Force Systems Command, Griffiss Air Force Base, NY 13441-5700.

Time-Dependent Failure Rates for Jet Aircraft by Maurice B. Shurman. From the Proceedings 1978 Annual Reliability and Maintainability Symposium. Pages 198-203.

Modeling Variable Hazard Rate Life Data by Richard Y. Moss, Corporate Reliability Engineering, Hewlett-Packard Co., 1501 Page Mill Road, Palo Alto, CA 94304, from the 28th Electronic Components Conference. Library of Congress Catalog No. 79-140963.

Weibull Calculated Failure Rates For MIL-C-39003 Revision F Solid Tantalum Capacitors, by Carl M. Roman, Union Carbide Corp., Electronics Division, P.O. Box 5928, Greenville, SC 29606. Evaluation Engineering Magazine, Sept, 1984.

Weibull Analysis Handbook, by Dr. R.B. Abernethy, J.E. Breneman, C.H. Medlin, G.I. Reinman; Pratt & Whitney Aircraft, Government Products Division, United Technologies Corp., P.O. Box 2901, West Palm Beach, FL 33402. November 1983. Listed under the numbers AD-A143 100 and AFWAL-TR-83-2079. Distributed through the Aero Propulsion Laboratory, AF Wright Aeronautical Laboratories, AF Systems Command, Wright-Patterson AFB, Ohio 45433.

COMPARISON OF TOOLS
CARE III, SURE & HARP

October 7, 1987

Anna L. Martensen

PRC Kentron, Inc.

GENERAL COMMENTS

Preceding each advantage or disadvantage is a rating in brackets. The following is a rating "key":

Advantage Rating	Disadvantage Rating
1 -- Biggest advantage	1 -- Biggest disadvantage
2 -- Major program advantage	2 -- Large or major deficiency
3 -- Worth mentioning	3 -- Deficiency worth mentioning
4 -- Barely worth mentioning	4 -- Barely worth mentioning

Each program is evaluated in near-isolation. For example, the fault tree capability in CARE III is listed as a "Major program advantage." The same capability in HARP, however, is one of the program's many advantages, and receives a "Worth Mentioning" rating.

Sal Bavuso's comments are shown in *ITALICS*
and Anna Martensen's comments are **BOLDED.**

NO CROSS-COMPARISON OF THE THREE PROGRAMS IS ATTEMPTED.

REQUIREMENTS

Several predefined Fault/Error Handling Models (FEHM) and possibly one user defined structured model. These models are used in conjunction with behavioral decomposition to reduce the model state size.

Large and/or arbitrary structured Markov chains

Markov chain generator

Weibull or nonconstant failure distributions

Work-station input with fault tree or Markov chain notation

Phased mission assessment

Performability computation and intermediate state probabilities

Parametric analysis capability

REQUIEMENTS (CONCLUDED)

Availability/reliability computation

Hot/cold spares

Reliability bounds computation

Computational accuracy estimates

Exact results or at least provably conservative results

Validated and extensively tested code

Machine portable code

Well written documentation

Computationally fast tools (less than 24 cpu hours for very large models)

CARE III Strengths

(1) **Large models that can be described by a fault tree can be modeled with the CARE III program**

(2) **The fault tree description of the system provides a concise method for describing the system**

(2) **Intermediate state probabilities can be examined by selecting the appropriate print option**

(3) **Some systems with Weibull failure processes can be modeled**

(2) Most systems with Weibull failure processes can be modeled; some cannot

(4) **There is a limited hot spare capability**

( ) Engineering oriented interface

( ) **Powerful general single fault handling model**

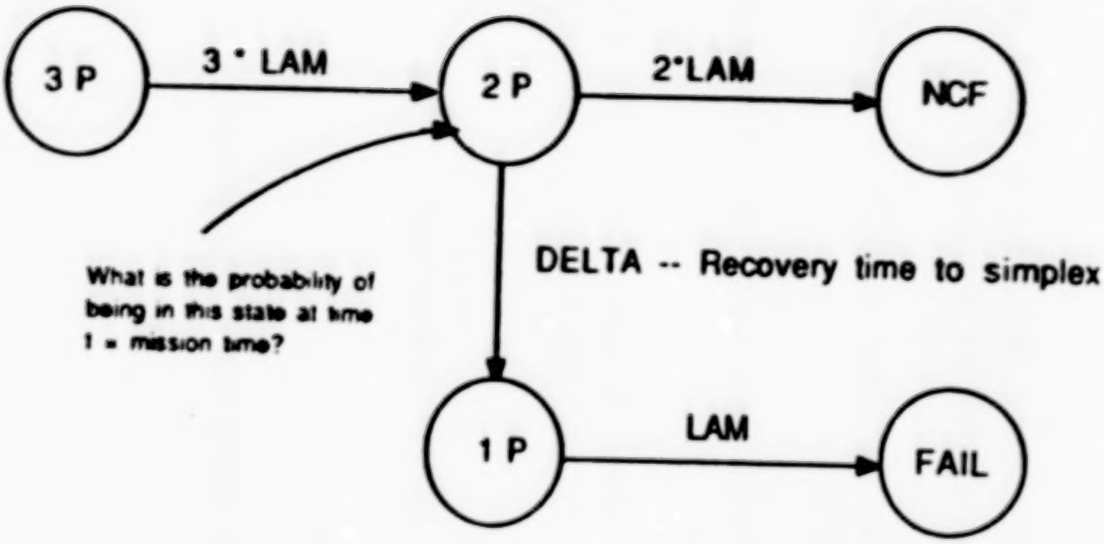


Figure 1. Intermediate state model

CARE III Weaknesses

(1) **No state dependent transitions are allowed. This therefore precludes cold spares, "warm" spares, or changing fault handling characteristics**

(2) **Spares must assume the same fault/error handling model as on-line units**

(2) **Systems with repair cannot be modeled**

Systems with instantaneous repair cannot be modeled. Steady state repair is possible

(2-3) **No indication of the level of conservativeness is provided**

(2-3) **No automatic parametric analysis capability is provided**

(4) Automatic parametric analysis is easily accomplished with DEC command language statements.

(3) **List directed input is very difficult to use**

(3) **The CARE III Weibull capability is limited by the constraints listed above: no repair or state dependent transtions.**

(4) **Critical m-tuples, m >= 3, cannot be modeled**

ORIGINAL PAGE IS
OF POOR QUALITY

HARP Strengths

(2) *(1)* The program provides a reasonably flexible Markov capability, especially for systems that can be decomposed to FORM and FEHM

(2) Systems with repair can be modeled

(2) There are several ways to describe fault handling data

(2) Intermediate state probabilities can be examined

(2-3) *(2)* The state reduction due to behavioral decomposition can be extensive

(2-3) HARP has an automatic parametric analysis capability

(3) *(2)* Some *(many)* systems with Weibull failures can be modeled

(3) Conservativeness of the decomposition/aggregation technique for the homogeneous case has been proven and published

(3) *(2)* The automatic generation of a Markov chain from a fault tree description can be a valuable tool

(3) HARP input files are easily edited by hand

ORIGINAL PAGE IS
OF POOR QUALITY

HARP Strengths (cont.)

- ( ) *Computation of reliability bounds - the "real" value theoretically lies between the bounds*
- ( ) *Computation of global error bounds*
- ( ) *Computation accuracy of typically greater than 12 digits*

HARP Weaknesses

(1) Not all arbitrary homogeneous and non-homogeneous Markov models can be modeled

(2) *(3)* To solve some systems, "work arounds" must be used

(2-3) No independent verification of the math or code

(2-3) No indication of the level of conservativeness is provided

(3) The Weibull capability must be used with caution when modeling spares

(3) The user interface is functional, but far from glamorous

(4) Critical m-tuples, m >= 3, cannot be modeled

( ) *Weibull computations are slow*

( ) *No warning is given when behavioral decomposition assumptions are violated*

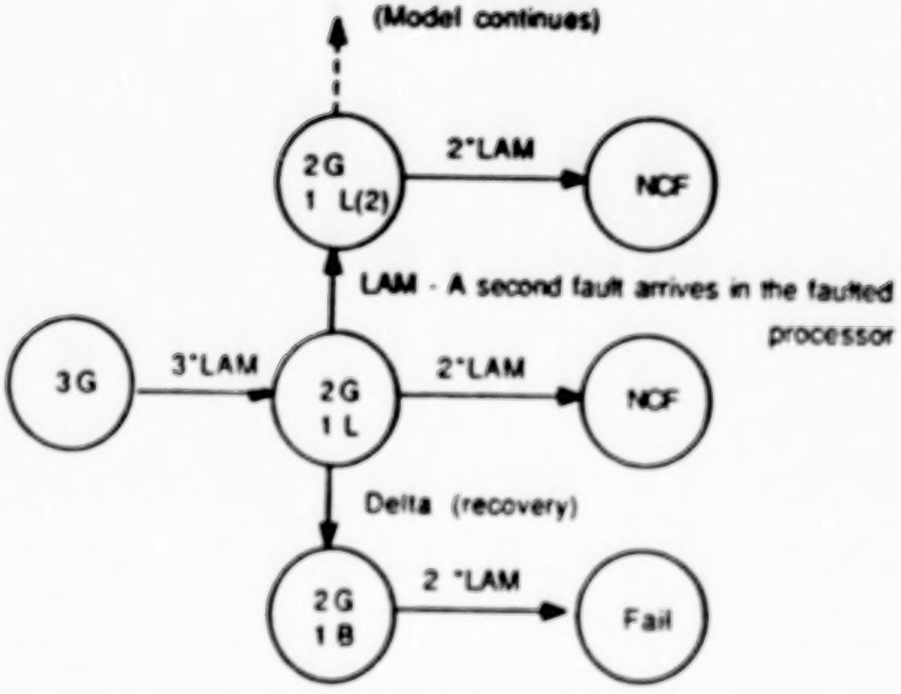


Figure 2. An arbitrary Markov model

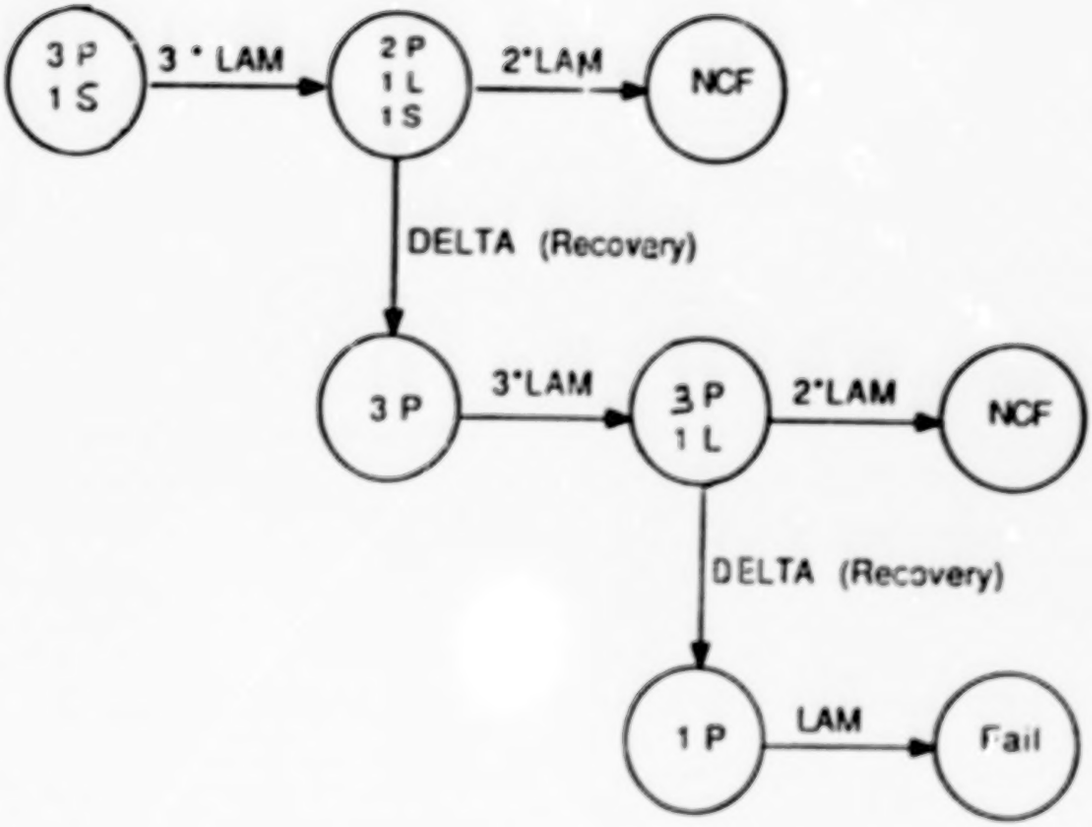


Figure 3. Cold spare model

SURE Strengths

(1) Any arbitrary model, subject to (1) slow transions are exponentia ("slow": rate x time < 0.1); (2) the means and variances of the fast transitions are less than the mission time; and (3) "fast loops" are not modeled

(2) Simple, rigorous mathematical basis

(2) "Real" system unreliability lies between the SURE bounds

(2) Nice parametric analysis capability

(2) Input language is clean, easily understood, simple to use. Without ASSIST, though, generation of large models (100+ states) is virtually impossible

(3) Repair can be modeled

(3) Fault handling and recovery are easily enumerated with the semi-Markov mean and variance

(4) Critical m-tuples can be modeled, m >= 2

SURE Weaknesses

(2) Not suitable for medium to large systems with detailed fault handling mechanisms

(2) Weibull fault-occurrences cannot be modeled directly

(3) "Fast looping" transition paths may defeat the SURE mathematics

(3) *(1)* Only death state probabilites may be examined

(3) *(2-3)* Mathematics and code have not been independently verified. An in-house testing effort has been performed.

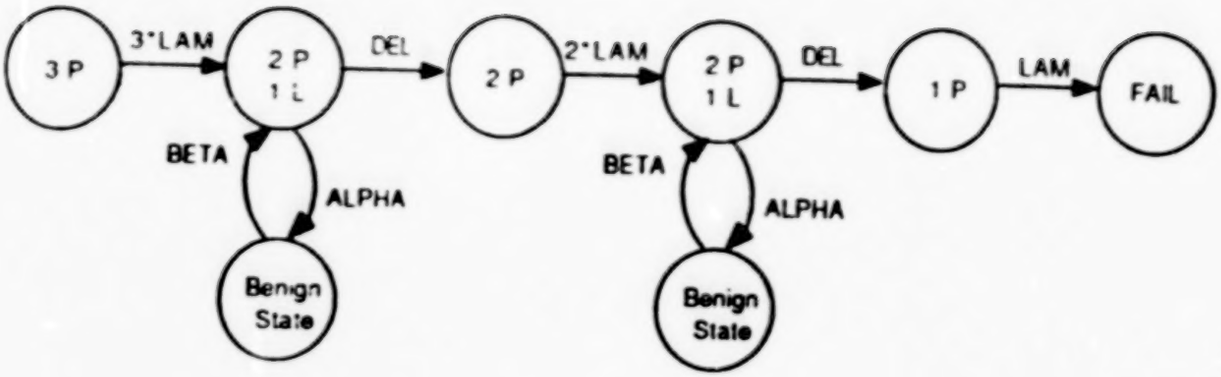


Figure 4. Intermittent fault model

INTRODUCTION TO THE CARE III WORKSHOP

October 6, 1987

Salvatore J. Bavuso

NASA Langley Research Center

STATEMENT OF WORK

DEVELOPMENT OF A GENERAL
COMPUTER-AIDED-RELIABILITY
ESTIMATION TECHNIQUE
(CARE III)

1-05-1551.0282
Exhibit A

February 7, 1977

NASA — LANGLEY RESEARCH CENTER —
HAMPTON, VA
23665

applied to three advanced fault tolerant systems as a check on the model's flexibility and accuracy. Requirements for a user-oriented computer program which embodies the CARE III reliability modeling technique, will also be generated. In the second phase, the CARE III model user-oriented computer program shall be written and tested.

2.0 STUDY OBJECTIVE

The objective of this study is to develop a general reliability assessment technique which is capable of estimating the reliability of a broad class of fault-tolerant computer and digital flight control systems. In its final form, the advanced technique will be implemented as a user-oriented computer program.

3.0 CONTRACTOR TASKS

The contractor shall perform the following tasks in two phases of work: Phase I shall include task 3.1 (establish the requirements for a general reliability assessment tool), task 3.2 (develop the CARE III reliability modeling technique), and task 3.3 (demonstrate and validate the CARE III technique). Phase II shall include task 3.4 (generate a user-oriented CARE III computer program).

3.1 Requirements for General CARE III Capability

3.1.1 General CARE Assessment Technique

The contractor shall determine the requirements for a general CARE assessment technique. The selected requirements should be broad enough to encompass both present and anticipated digital computer,

flight control systems, and assessment techniques. Detail examination of these systems and techniques should provide a sound basis for determining the requirements. A partial list of requirements is identified in 3.1.1.2. The union of these listed requirements and those generated by the contractor should establish a sufficient set of requirements.

3.1.1.1 The contractor shall study at least the following techniques for determining the requirements: CARE II (Computer-Aided Reliability Estimation), CAST (Combined Analytic Simulative Technique), CARSRA (Computer-Aided Redundant System Reliability Analysis), the SIFT (Software Implemented Fault-Tolerant) Computer Semi-Markov Technique, the Markov Technique utilized to assess the CSDL (Charles Stark Draper Laboratory) parallel Hybrid Multiprocessor, the modeling techniques utilized for the U.S. Air Force's Fault-Tolerant Spaceborne Computer (FTSC). The contractor shall also examine the following computer systems in determining CARE III requirements: ARCS (Advanced Reconfigurable Computer System), SIFT, CSDL Parallel Hybrid Multiprocessor, the FTSC, and the WMCS (whole Word Computer System).

3.1.1.2 The contractor shall consider at least the following items for inclusion in the requirements:

3.1.1.2.1 Reliability Structural Model

- o coverage parameters
- o Poisson and non-Poisson transient fault parameters and/or models with renewal (self-repair)
- o Poisson and non-Poisson software fault parameters and/or models
- o Poisson and non-Poisson hardware fault parameters and/or models

ORIGINAL PAGE IS
OF POOR QUALITY

+ o general fault redundancy management capability and systems success criteria

+ o utilization of standard reliability models such as TMR and stand-by

+ o functional dependency between stages

— o sensitivity analysis capability

? o amenable to validation

3.1.1.2.2 Coverage Model

I o cover all important fault classes (e.g. hardware, software, transient, and latent) and coverage enhancement mechanisms (fault detectors, isolators, and reconfiguration schemes)

+ o compatible with the general reliability structural model (3.1.1.2.1)

? o uses available or measurable input data

+ o time dependent coverage

? o amenable to validation

3.1.2 General CARE Computer Program Requirements

The contractor shall determine the requirements for the computer program that shall implement the General CARE technique and shall include at least the following:

+ o user-oriented (batch or interactive)

? o easy to operate, set up, and manipulate

+ o reasonable operational costs and accuracy

3.2 Development of a General Reliability Technique (CARE III Technique)

3.2.1 CARE III Model

ORIGINAL PAGE IS
OF POOR QUALITY

3.2.1.1 The contractor shall examine various modeling techniques to meet the requirements established under task 3.1. The methods to be considered shall include, but shall not be limited to, direct extensions of the CARE II model with or without additional constraints, use of Laplace transforms to eliminate multiple integrals, and a generalized Markov-chain analysis based on the Chapman-Kolmogorov constraint.

3.2.1.2 The CARE III Model shall accommodate the following:

- o number of stages shall be at least 40
- o number of modes shall be N, where N is user assignable. N-point failure N = 1, 2 This capability shall allow multiple dependencies across stages.
- o a non-recoverable module transient should not cause system failure, but shall be treated as a "leaky" transient as a user option.

3.2.2 CARE III Coverage Model

3.2.2.1 The contractor shall enhance the CARE II coverage model to meet the requirements established under task 3.1.

3.2.2.2 The contractor shall identify and develop techniques to simplify the task of acquiring data for the coverage model.

3.3 Demonstration and Validation of the CARE III Technique

The contractor shall assess at least the ARCS, SIFT, WMCS, and Parallel Hybrid Multiprocessor Computer/Flight Control Systems utilizing the CARE III technique and compare these results with published assessment results for these systems.

3.4 User-Oriented General Reliability Estimation Computer Program (CARE III)

NASA CONTRACTOR REPORT 159122

CARE III FINAL REPORT

PHASE I

VOLUME I

J. J. Stiffler, L. A. Bryant, L. Guccione

RAYTHEON COMPANY
SUDBURY, MASSACHUSETTS 01776

PREPARED UNDER
NASA CONTRACT NAS1-15072

FOR
NASA LANGLEY RESEARCH CENTER
HAMPTON, VIRGINIA

AIR FORCE AVIONICS LABORATORY
WRIGHT PATTERSON AIR FORCE BASE, OHIO

NOVEMBER 1979

ORIGINAL PAGE IS
OF POOR QUALITY

National Aeronautics and Space Administration
Langley Research Center
Hampton, Virginia 23665

ORIGINAL PAGE IS
OF POOR QUALITY

interconnected by seven different bus networks (address bus, data bus, control bus, power bus, timing bus, interrupt bus, status bus). Each of these elements and buses is provided with redundant spares, in various configurations depending upon its complexity. (One element, the memory module, is itself internally redundant as well.)

The current FTSC reliability model is a simplified, one-mode, sixteen-stage version of CARE II. In some cases, non-unity dormancy factors were used to account for the lower failure rate of inactive and unpowered modules.

2.2 CARE III REQUIREMENTS

The emphasis in the previous section was on the techniques used to estimate the reliabilities of the systems in question. At a minimum, CARE III must provide a unified model for all four of those systems and hence reproduce, under the appropriate set of conditions, the results obtained using each of these models. This, of course, is a necessary but not a sufficient condition to place on CARE III. To be most useful, it must be flexible enough to overcome any limitations imposed by the above models (e.g., restrictive coverage models, limited fault models, etc.) and at the same time sufficiently general to allow other, as yet unspecified, fault-tolerant systems to be modeled without introducing artificial restrictions. The following paragraphs outline the requirements imposed on CARE III and explain the rationale for each of these requirements in terms of the above objectives.

+ 1. Capability of modeling up to at least 40 stages.

Rationale: This is specified in the CARE III Statement of Work. Although none of the systems considered in paragraph 2.1 require as many as 40 stages, it is not difficult to conceive of systems that do. This requirement will be satisfied in CARE III by providing a means for concatenating independent

runs. If the coupling between stages is limited, it will in fact be possible to model an arbitrarily large number of stages by making repeated runs.

— 2. Multiple operating modes for each set of coupled stages. State dependent coverage

Rationale: The operating mode of a system or subsystem is, so far as its reliability model is concerned, a function of its structure (number of units of various types that have to be operational for the system to function as specified) and its coverage parameters. If the system's structure or coverage coefficients change stochastically during its operating lifetime (e.g., if they depend upon the number of faults already incurred) such changes must be reflected in its reliability model. If a mode change in one stage precipitates a mode change in some other stage, the two stages are said to be coupled. (Deterministic structural or coverage parameter changes must, of course, also be reflected in the reliability model. Such changes are relatively easily accommodated, however, by introducing time-dependent coverage parameters and by concatenating reliability models representing the disjoint time intervals during which the system structure is invarient. Thus, such mode changes impose no new constraints provided only that the coverage parameters are allowed to be time-dependent.)

CARE II allowed only one mode change (two operating modes); the exhaustion of the spares available at any one stage could cause the system to change from, say, a dual-redundant to a single-string configuration, thereby changing both the system structure and the coverage coefficients associated with each stage. Two of the systems discussed in paragraph 2.1, however,

ORIGINAL PAGE IS
OF POOR QUALITY

(SIFT and ARCS) exhibited mode changes after each new fault. Thus, the two-mode limitation of CARE II is not acceptable for CARE III.

+ 3. Separate coverage model similar to that in CARE II but capable of handling latent and intermittent faults as well as permanent faults.

Rationale: The major advantage in keeping the reliability and coverage models distinct (as they were in CARE II) is that it allows the user to concentrate on each of these two areas relatively independently and hence simplifies the task of defining the system model. In addition, there are some significant practical advantages (cf. Section 4) in separating the reliability model, driven by infrequently occurring failures, from the coverage model reflecting the much more rapid detection, isolation and recovery events.

The need to handle both intermittent and latent faults in the coverage model is evident from the discussion in paragraph 2.1.

+ 4. Multiple success criteria

Rationale: As ARCS clearly demonstrates, some redundant systems may be considered operational under any one of a number of possible conditions. It is therefore necessary for the user to be able to define each of those conditions and for CARE III to calculate the probability that at least one of them occurs.

± 5. $n = 1, 2$ n-point failure mechanisms ("category 3" faults)

Rationale: Most fault-tolerant systems exhibit "n-point-failure" mechanisms; i.e., sets of n failures ($n \geq 1$) that can disable the system even though spare hardware is available. If two BGU's fail in the enable mode in the FTMP, for example,

ORIGINAL PAGE IS
OF POOR QUALITY

the system is potentially inoperative even though spare operational modules are available. CARE II modeled such failure mechanisms only for n = 1. Although the probability of such failures is generally a rapidly decreasing function of n, it cannot a priori be considered negligible for all n > 1. The concept of a single-point failure must therefore be generalized to take this into account.

+ 6. Time-dependent hazard rates

Rationale: All of the reliability models considered in paragraph 2.1 assumed constant hazard rates. There are at least two reasons why it would be desirable to relax this restriction: (1) Recent data indicate that at least in some environments (space) the hazard rates are far from constant. (2) The hazard rates associated with modules having internal redundancy are not constant even if the individual component hazard rates are.

+ 7. Transient faults

Rationale: Most faults are modeled either as permanent or intermittent, the latter actually being permanent faults that manifest themselves intermittently. Some faults may well be transient in nature, however; e.g., faults due to noise or those due to improperly validated software. In such cases, no hardware damage has occurred and, as soon as the cause of the fault disappears, the system can, in principle, function as before.

— 8. Non-unity dormancy factors

Rationale: Of the four models discussed in paragraph 2.1, only the FTSC model allowed non-unity dormancy factors. In some cases, it is reasonable to assume that dormant (e.g., unpowered or inactive) modules may have lower hazard rates

REQUIREMENTS

± - Several predefined Fault/Error Handling Models (FEHM) and possibly one user defined structured model. These models are used in conjunction with behavioral decomposition to reduce the model state size.

± - Large and/or arbitrary structured Markov chains

? - Markov chain generator

+ - Weibull or nonconstant failure distributions

– - Work-station input with fault tree or Markov chain notation

– - Phased mission assessment

± - Performability computation and intermediate state probabilities

– - Parametric analysis capability

REQUIEMENTS (CONCLUDED)

± - Availability/reliability computation

± - Hot/cold spares

– - Reliability bounds computation

— - Computational accuracy estimates

± - Exact results or at least provably conservative results

+ - Validated and extensively tested code

+ - Machine portable code

? - Well written documentation

+ - Computationally fast tools (less than 24 cpu hours for very large models)

CARE III EVOLUTION

1977	SOW
1982-84	CARE III, VERSION 4, CDC FORTRAN IV, RELEASED TO COSMIC
	CARE 3 MENU PROGRAM WRITTEN FOR 1984 WORKSHOP
1985	CARE III, VERSION 5, VAX FORTRAN 77 , CDC FORTRAN V
1986	BEGIN BETA TESTING OF VERSION 6

- CURRENTLY 30 + BETA TEST SITES FOR ALL VERSIONS
- CARE 3 MENU UPDATED AND ENHANCED, VERSION 6 COMPATIBLE

ORIGINAL PAGE IS
OF POOR QUALITY

AGENDA

CARE III Users' Workshop, October 6-7, 1987

Co-Chairmen: Salvatore J. Bavuso, NASA Langley Research Center
Anna L. Martensen, PRC Kentron, Inc.

Tuesday

Welcome: Sal Bavuso, Workshop Co-Chairman Division Representative;
Chuck Meissner, Branch Head SVMB
Introduction to the CARE III Workshop: Sal Bavuso
Introduction to the CARE III Mathematical Model: Roberto E. Altschul
The CARE III Implementation and Code: Anna L. Martensen
RTI's Use of CARE III: Charlotte Scheper
USE of CARE III for Flight Controls Development
at Northrop: Jack Flynn

Wednesday

Questionnaire Review and Discussion: Sal Bavuso
CARE III Model — User's Overview: John Sight
Examples of Nonconservative Reliability Estimates
Given by CARE III: Kelly J. Dotson
Comparison of Tools (CARE III, SURE, HARP): Anna L. Martensen
Demonstrations in AIRLAB:
Overview: Chuck Meissner
The Semi-Markov Unreliability Range Evaluator (SURE): Ricky Butler
Fault Injection: George Finelli
Software Reliability: Jon Sjogren
HARP: Sal Bavuso
CARE III and HARP Hands-On Demonstrations and Tutorials
Weibull References

CARE III USERS' WORKSHOP ATTENDEES AND THEIR ADDRESSES

October 6-7, 1987

Name	Job Title	Address
Charlotte Scheper (919) 541-7116	Comp. Scientist	Research Triangle Institute PO Box 12194 Research Triangle Park, NC 27709
Jack Flynn (213) 940-5076	Sr. Tech. Spec.	Northrop Corporation E294/6A 8900 E. Washington Blvd. Pico Rivera, CA 90660
Don Lee (213) 366-4366	MTS	The Aerospace Corp. M/S M1/166 2350 El Segundo Blvd. El Segundo, CA 90245
Jocelyn Frosch (817) 763-3278	Engineer	General Dynamics Ft. Worth Division PO Box 748 MZ 2660 Ft. Worth, TX 76101
Fred Swern (201) 420-5582	Professor	Stevens Institute of Technology Dept. of Mechanical Engineering Hoboken, NJ 07030
Lori Bechtold (206) 773-8613	Engineer	Boeing Aerospace Co. M/S 82-15 PO Box 3999 Seattle, WA 98124-2499
Ha Vuong	Engineer	Boeing Aerospace Co. M/S 82-15 PO Box 3999 Seattle, WA 98124-2499
David DeLorm (617) 276-2517	Rel. Eng.	ITEK Optical Systems 10 Maguire Rd Lexington, MA 02173

Name	Job Title	Address
Robert P. Landstrom (617) 440-2019	Sr. Eng.	Raytheon Co., Equipment Div. 528 Boston Post Rd. Sudbury, MA 01776
Don Livaccari (516)346-2270	Sr. Eng.	Grumman Space Systems M/S A02-105 Bethpage, NY 11714
Wah Ng (516) 346-2887	Rel. Eng.	Grumman ASD M/S K03-14 Bethpage, NY 11714
Peter Yip (516) 346-2888	Rel. Eng.	Grumman ASD M/S K03-16 Bethpage, NY 11714
Jacob Shuker	Sen. Eng.	Grumman Space Systems Div. M/S A02-105 Bethpage, NY 11714
Johnny Sight (213) 332-0367	Engineer II	Northrop Corporation Aircraft Div. M/S 1834/90 One Northrop Ave. Hawthorne, CA 90250
James F. Eck (213) 594-3218	MTS 6	Rockwell International 2600 Westminster Blvd. Mail Code SK54 Seal Beach, CA 90740-7644
Robert Villet (213) 594-3218	MTS 6	Rockwell International Box 3644 Mail Code SK54 Seal Beach, CA 90740-7644
Kurt A. Liebel (602) 869-2837	Sen. Proj. Eng.	Honeywell, Inc. Sperry Comm. Flt. Sys. Group PO Box 2111, MS 020C4 Phoenix, AZ 85036
Roberto E. Altschul (206) 865-3031	Res. Eng.	Boeing Electronics Co. PO Box 24969 MS 7J-27 Seattle, WA 98124-6269
Jerry Bilyk	Unit Chief	McDonnell-Douglas Corp. Box 516 Bld. 065, L4W, 303 St. Louis, MO 63166

NASA National Aeronautics and Space Administration

Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
NASA CP-10011		

4. Title and Subtitle	5. Report Date
CARE III Users' Workshop	April 1988
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Research Triangle Institute, Compiler	
	10. Work Unit No. 505-66-21-02

9. Performing Organization Name and Address	11. Contract or Grant No.
NASA Langley Research Center Hampton, VA 23665-5225	
	13. Type of Report and Period Covered: Conference Publication

12. Sponsoring Agency Name and Address	14. Sponsoring Agency Code
National Aeronautics and Space Administration Washington, DC 20546-0001	

15. Supplementary Notes

This publication consists mainly of viewgraphs.

16. Abstract

A user's workshop for CARE III, a reliability assessment tool designed and developed especially for the evaluation of high-reliability fault-tolerant digital systems, was held at NASA Langley Research Center on October 6-7, 1987. The main purpose of the workshop was to assess the evolutionary status of CARE III.

This report documents the activities of the workshop and includes papers by user's of CARE III and NASA. Features and limitations of CARE III and comparisons to other tools are presented. The conclusions to a workshop questionnaire are also discussed.

17. Key Words (Suggested by Author(s))	18. Distribution Statement
CARE III Reliability Fault Tolerant Coverage Fault Handling	Unclassified - Unlimited Star Category 59

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of pages	22. Price
Unclassified	Unclassified	159	A08

NASA FORM 1626 OCT 86

For sale by the National Technical Information Service, Springfield, Virginia 22161-2171

END

DATE

FILMED

JUL 8 1988